

NAVAL POSTGRADUATE SCHOOL

Monterey, California



THESIS



**A Framework for Evaluating Application of Smart
Cards and Related Technology Within the
Department of Defense**

by

Joseph Brian Spegele

September, 1994

Co-Advisors:

Carl R. Jones
Dan C. Boger
Roger Stemp

Approved for public release; distribution is unlimited.

DTIC QUALITY INSPECTED 3

19950117 025

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.				
1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE 1994, September		3. REPORT TYPE AND DATES COVERED Master's Thesis
4. TITLE AND SUBTITLE A Framework for Evaluating Application of Smart Cards and Related Technology Within the Department of Defense			5. FUNDING NUMBERS	
6. AUTHOR(S) Spegele, Joseph Brian				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)			10. SPONSORING / MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the authors and do not necessarily reflect the official policy or position of the Department of Defense or the U.S. Government.				
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.			12b. DISTRIBUTION CODE A	
13. ABSTRACT (Maximum 200 words) The author presents a new framework for evaluating the evolutionary upgrade paths of card technologies. Many functions which are now either not being done, or are being done manually, could be automated using card technologies. There is a revolution underway in card technologies, making them viable solutions to an expanding set of problems. The author examines these card technology initiatives, the shrinking defense budget, card selection issues, card authentication techniques, and evolutionary acquisition. Conclusions stress that card technology systems can be viewed as evolutionary upgrade paths that change over time. Simple cost benefit analysis does not capture the evolving nature of advancing technology. Effective evaluations of evolutionary card systems must consider this temporal component, and a framework, such as the one presented in this thesis, is needed for comparing alternative card systems.				
14. SUBJECT TERMS Smart cards, Card technology, Evolutionary acquisition, Migration, Migratory systems			15. NUMBER OF PAGES 194	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UL	

Approved for public release; distribution is unlimited.

A Framework for Evaluating Application of Smart Cards and Related Technology
Within the Department of Defense

by

Joseph B. Spegele
Lieutenant, United States Navy
B.S., United States Naval Academy, 1988

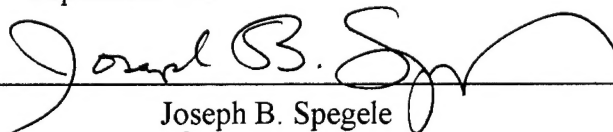
Submitted in partial fulfillment
of the requirements for the degree of

**MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT
and
MASTER OF SCIENCE IN MANAGEMENT**

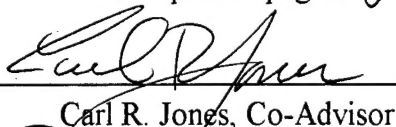
from the

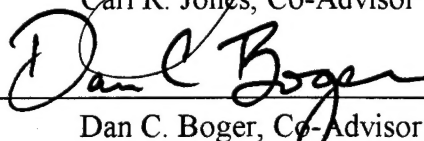
NAVAL POSTGRADUATE SCHOOL
September 1994

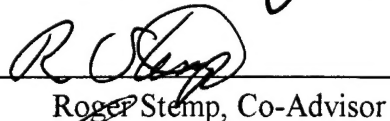
Author:

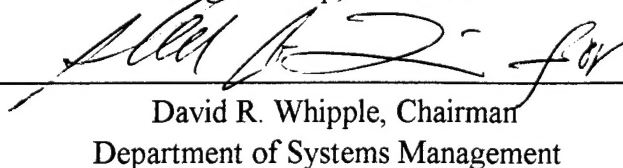

Joseph B. Spegele

Approved by:


Carl R. Jones, Co-Advisor


Dan C. Boger, Co-Advisor


Roger Stemp, Co-Advisor


David R. Whipple, Chairman
Department of Systems Management

ABSTRACT

The author presents a new framework for evaluating the evolutionary upgrade paths of card technologies. Many functions which are now either not being done, or are being done manually, could be automated using card technologies. There is a revolution underway in card technologies, making them viable solutions to an expanding set of problems. The author examines these card technology initiatives, the shrinking defense budget, card selection issues, card authentication techniques, and evolutionary acquisition.

Conclusions stress that card technology systems can be viewed as evolutionary upgrade paths that change over time. Simple cost benefit analysis does not capture the evolving nature of advancing technology. Effective evaluations of evolutionary card systems must consider this temporal component, and a framework, such as the one presented in this thesis, is needed for comparing alternative card systems.

Accession For	
NTIS	CRA&I <input checked="" type="checkbox"/>
DTIC	TAB <input type="checkbox"/>
Unannounced	<input type="checkbox"/>
Justification	
By	
Distribution /	
Availability Codes	
Dist	Avail and / or Special
A-1	

TABLE OF CONTENTS

I. INTRODUCTION	1
A. PURPOSE OF THESIS	1
B. SCOPE AND METHODOLOGY	3
C. OUTLINE OF CHAPTERS	4
1. Chapter II Technology Performance Issues	4
2. Chapter III Card Technology Overview	4
3. Chapter IV Authentication Techniques.	4
4. Chapter V New Framework Background	4
5. Chapter VI A Framework For Card Selection	5
6. Chapter VII Conclusions And Recommendations.	5
II. TECHNOLOGY PERFORMANCE ISSUES.	6
A. INTRODUCTION.	6
B. BACKGROUND ON CARD SYSTEM PERFORMANCE ISSUES.	6
C. DISCUSSION OF ISSUES	9
1. Security Requirements	9
a. Level of Security Required Considerations	9
b. Types of Security	10
c. Error Tolerance Considerations.	11
2. Memory Requirements	13
a. Amounts of Data to be Stored	13
b. Speed of Data Transfer.	16
c. Data Storage Characteristics	16
3. Processing Requirements	17
4. Interface Requirements	18
5. Durability	19
a. Durability of Cards and of Card Interface.	19
b. Durability of Card Readers and Authenticating Devices.	20
6. User Acceptance	20
a. Acceptance of Authentication Technique	21
b. Acceptance of Card Technology.	21
7. Scalability and Expandability	22
8. Application Specific Attributes	22
9. System Life Expectancy	23
10. Cost Estimations	23
a. Reuse of Current Infrastructure	24
b. Cost Estimation.	25

c. Acquisition and Procurement	25
d. Hardware and Software	26
e. Data Capture	27
f. Operations and Maintenance	27
g. Training	27
h. Application Specific Costs	28
11. Risk Assessment	28
12. Temporal Component.	29
D. CONCLUSION	29
III. CARD TECHNOLOGY OVERVIEW	30
A. INTRODUCTION	30
B. HISTORY OF CARD EVOLUTION	30
C. CARD TECHNOLOGIES.	34
1. Bar Codes	34
a. History	34
b. System Descriptions	35
(1) Code 39 Bar Code	36
(2) Code 128 Bar Code	37
(3) Universal Product Codes (UPC)	38
(4) Interleaved 2 of 5	38
(5) Code 49	39
(6) Code 16K	39
(7) Other Symbolologies	40
c. Common Applications	40
d. Capabilities	41
e. Limitations	41
2. Magnetic Stripe	42
a. History	42
b. System Description	42
c. Common Applications	44
d. Capabilities	45
e. Limitations	45
3. Wiegand Technology Cards	46
a. History	46
b. System Description	46
c. Common Applications.	47
d. Capabilities	48
e. Limitations	48
4. Integrated Circuit Cards	49
a. Background	49
b. Evolution of the IC Card	52

c. Contact Chip Cards	54
(1) System Description	54
(2) IC Programmable Cards	54
(a) Common Applications.	55
(b) Capabilities	56
(c) Limitations	57
(3) IC Memory Cards	58
(a) Common Applications.	58
(b) Capabilities	59
(c) Limitations	59
(4) Super Smart Cards.	59
(a) Common Applications.	60
(b) Capabilities	60
(c) Limitations	61
d. Contactless Chip Cards	61
(1) System Description.	61
(2) IC Programmable Cards	62
(a) Common Applications.	62
(b) Capabilities	63
(c) Limitations	64
(3) IC Memory Cards.	64
(a) Common Applications.	65
(b) Capabilities	65
(c) Limitations	65
e. PCMCIA	66
(1) System Description.	66
(2) Common Applications	67
(3) Capabilities.	67
(4) Limitations	67
5. Optical Memory Cards	68
a. History	68
b. System Description	69
c. Common Applications	69
d. Capabilities	70
e. Limitations.	71
6. Hybrid Technology	71
a. History	71
b. System Description	72
c. Common Applications	73
d. Capabilities	73
e. Limitations.	73
D. SUMMARY	74

IV. AUTHENTICATION TECHNIQUES	76
A. INTRODUCTION	76
B. BACKGROUND	77
C. AUTHENTICATION BY HUMAN INTERVENTION (MANUAL)	82
1. Authentication of the Individual	82
a. Photograph	82
b. Signature Block	83
2. Authentication of the Access Device	84
a. Name Embossing	84
b. Holographic Seals and Images	84
D. AUTHENTICATION BY MACHINE (AUTOMATED)	85
1. Authentication of the Individual	85
a. Personal Identification Number or Password	85
(1) Fixed	85
(2) Challenge and Response Systems	85
b. Physiological (Biometrics)	86
(1) Fingerprint	88
(2) Hand Geometry Recognition	89
(3) Retinal Scan	91
(4) Iris Scan	92
(5) Face Recognition	93
(6) Hand Vein Patterns	93
(7) Other Technologies	93
c. Behavioral	94
(1) Signature Dynamics Verification	94
(2) Keystroke Dynamics	95
(3) Voice Recognition	95
2. Authentication of the Access Device	97
a. Optical Character Recognition	97
b. Magnetic Ink	97
c. Electronically Verifiable Holograms	98
d. Cryptographic Techniques	99
e. Zero-Knowledge Authentication	102
E. SUMMARY OF AUTHENTICATION TECHNIQUES	103
V. NEW FRAMEWORK BACKGROUND	104
A. INTRODUCTION	104
B. EVOLUTIONARY MIGRATION CONCEPT	104
C. DEPARTMENT OF DEFENSE SUPPORT	105
1. National Performance Review	105
2. Corporate Information Management	106

3. Command, Control, Communications, Computers and Intelligence for the Warrior	108
4. DoD Directive 5000.1 and Instruction 5000.2	109
5. Technical Architecture for Information Management	110
D. THEORIES AND CONCEPTS	112
1. Analytical Hierarchy Process	112
2. Commercial-off-the-Shelf	113
3. Open Architecture	114
4. Discounting to Obtain Present Values	114
5. Cost Analysis Concepts	116
6. Risk Analysis Concepts	116
E. SUMMARY	117
VI. A FRAMEWORK FOR CARD SYSTEM SELECTION	118
A. INTRODUCTION	118
1. Framework Purpose and Problem Statement	118
2. The Need for an Effective Evaluation Framework	119
3. Methodology	120
B. THE FRAMEWORK	120
1. General Discussion	120
2. Overall Framework View	123
3. Framework Steps	125
a. Define Target System	125
(1) Determine Functions and Technical Capabilities	126
(2) Determine Current and Base System	127
(3) Determine System Life Expectancy of Current or Base System	128
b. Establish Migratory Paths	129
(1) List Current or Base Systems	130
(2) List Target System Attributes	130
(3) Construct Viable Paths to Target System	130
c. Develop and Apply Measures of Performance	132
(1) Determine Performance Attributes and Scales	132
(2) Use AHP to Develop an Aggregate Measure of Performance (MOP)	136
(3) Calculate the Aggregate MOP for Each Period	136
(4) Use AHP to Develop the Time Preference of Performance	137
(5) Calculate Overall Time Weighted MOP for Each Migration Path	137
d. Develop and Apply Hierarchical Cost Model	137
(1) Determine Cost Elements Drivers	138
(2) Develop Hierarchical Cost Model	139
(3) Calculate Costs for Each Period	139

(4) Discount Costs to Obtain the Present Values of Life Cycle Cost	139
(5) Calculate Present Value Life Cycle Cost for Each Migration Path	139
e. Calculate Overall Net Values	141
(1) Use AHP to Develop MOP and Life Cycle Costs Preferences	141
(2) Calculate Overall Net Values for Each Migration Path	142
f. Select Migratory Path	143
(1) Use Risk Analysis to Determine Likelihood of Path Occurrence	143
(2) Calculate Net Expected Value for Each Migration Path	144
(3) Select Path with Greatest Net Expected Value	144
g. Apply Selection and Reevaluate	144
(1) Initiate System Procurement	144
(2) Reevaluate New State Using Framework Steps	145
C. CONCLUSIONS	146
VII. CONCLUSIONS AND RECOMMENDATIONS	148
A. SUMMARY	148
B. CONCLUSIONS	148
C. RECOMMENDATIONS	149
APPENDIX A: LIST OF ACRONYMS	151
APPENDIX B: GLOSSARY	155
APPENDIX C: OTHER MOP SCALES	160
APPENDIX D: ILLUSTRATIVE EXAMPLE	163
BIBLIOGRAPHY	172
INITIAL DISTRIBUTION LIST	180

LIST OF FIGURES

Figure 1: Type I Vs. Type II Error Relationship	12
Figure 2: Code 39 Bar Code	37
Figure 3: Code 128 Bar Code	37
Figure 4: Universal Product Code	38
Figure 5: Interleaved 2 of 5 Bar Code	39
Figure 6: Code 49 Bar Code	40
Figure 7: Magnetic Stripe Card	45
Figure 8: ICC Technologies Hierarchy	51
Figure 9: Contact Chip Card	54
Figure 10: Super Smart Card	60
Figure 11: Contactless IC Card, Interior View	63
Figure 12: Optical Memory Card	69
Figure 13: Hybrid Technology Card, Front and Back	72
Figure 14: Authentication Hierarchy	79
Figure 15: Typical Encryption and Decryption Scheme	100
Figure 16: Cost Performance Decision Curve	121
Figure 17: The Steps of the New Framework	124
Figure 18: The New Framework - Step 1: Define Current and Target Systems . .	125
Figure 19: The New Framework - Step 2: Establish Migratory Paths	129

Figure 20: Migration Paths	131
Figure 21: The New Framework - Step 3: Develop and Apply MOP	132
Figure 22: Measures of Performance Hierarchy	134
Figure 23: The New Framework - Step 4: Develop and Apply Cost Model	138
Figure 24: Cost Model Hierarchy	140
Figure 25: The New Framework - Step 5: Calculate Overall Net Values	141
Figure 26: The New Framework - Step 6: Select Migratory Path	143
Figure 27: The New Framework - Step 7: Apply Selection, Periodically Review .	145
Figure 28: The New Framework Decision Hierarchy	147

LIST OF TABLES

TABLE 1: SUMMARY OF CARD TECHNOLOGIES	75
TABLE 2: SAMPLE FUNCTIONALITY VERSUS TECHNICAL CAPABILITY	127

I. INTRODUCTION

A. PURPOSE OF THESIS

Economists argue that in the decades since the great depression, *technology* has been responsible for between two-thirds and three-quarters of all U.S. productivity growth.¹ *Technology* can be defined as the "aggregation of capabilities, facilities, skills, knowledge, and organization required to successfully create a useful service or product."² The potential gains from technology are considerable. According to the Clinton administration's plan to reinvent government, information technology will play a central role in streamlining federal bureaucracy.³ To provide citizens with increased service at lower cost, the government needs to turn to new technology to reduce the needed human capital in the cost equation.⁴ *Smart cards* are one of the new technologies in the Clinton strategy.⁵ Smart card technologies can permit significant shifts in the amount and method of

¹ Solow, Robert, as quoted in Allison, Graham and Gregory, Treverton, (eds.), Rethinking America's Security: Beyond Cold War to New World Order, W.W. Norton and Co., NY, 1992, p. 120.

² Branscomb, Lewis M., et al., Empowering Technology: Implementing a U.S. Strategy, MIT Press, Cambridge, MA, 1993, p. 3.

³ Anthes, Gary H., "Feds to Downsize With IT," ComputerWorld, Vol. 27, No. 37, September 13, 1993, p. 16.

⁴ Toregas, Castis and Taly, Walsh, "Out With the Old, In With Re-engineering," American City & County, Vol. 108, No. 6, May 1993, p. 49.

⁵ Dreifus, Henry, "North American Smart Card Activities 1993," CardTech/SecurTech '93 Conference Proceedings, 1993, p. 353.

information which is acquired, stored, disseminated, and verified. Smart cards have the potential to revolutionize the way the Department of Defense (DoD) does business in many areas. They can centralize and automate functions which currently require expensive equipment, facilities, and personnel. The potential for even further productivity growth is obvious, and in this age of *right sizing* the force and tightening budget constraints, effective use of available technology is essential.

The purpose of this thesis is to present a new framework for evaluating alternative evolutionary upgrade paths for smart card related technologies. Card technology development advances, combined with decreasing DoD budgets and force structure, necessitate this emphasis on effective, efficient use of available technology. The problem of system selection is complicated by the fact that routine business must continue while the new technology is incorporated. The constant technology advances, need for interim systems, and difficulty in assessing overall systems capability cause the card selection process to be one of an evolutionary nature. Evolutionary Acquisition is an acquisition strategy which may be used to procure a system expected to evolve during development, within an approved architectural framework to achieve overall system capability. "An underlying factor in Evolutionary Acquisition is the need to field a well defined core capability quickly in response to a validated requirement, while planning through an incremental upgrade program to eventually enhance the system to provide overall system capability."⁶

⁶Hirsch, Edward, BGen., USA (Ret.), "Evolutionary Acquisition of Command and Control Systems: Becoming a Reality," Signal, Vol. 42, No. 5, January 1988, p. 23.

Evolutionary acquisition is well supported throughout the DoD, and will be discussed in depth in Chapter V.

This framework of evaluating possible card technology uses is not all inclusive. The possible combinations of technology to requirements is limitless, constantly changing and constrained only by the designer's imagination. This framework will provide the decision maker with the tools necessary to evaluate candidate technological solutions. This thesis also provides the decision maker with background on the current state of card technology, authentication schemes, and card selection issues.

B. SCOPE AND METHODOLOGY

The main focus of this thesis is to present a useful framework for evaluating evolutionary upgrade paths for card technology systems. To accomplish this it is necessary to present a review of issues surrounding card technology selection, the state of card technologies currently, and authentication techniques. This background is accomplished in Chapters II, III, and IV respectively. While this is not intended to be the definitive history, current state and future predictions of card technologies, it does serve as a thorough introduction to those not previously exposed to card technologies. To clarify concepts presented in the framework, an illustrative example is provided.

A major issue the framework addresses is the difficult, ever-present temporal component of card systems. The author proposes that effective evaluations of card technology systems must include an evaluation of its planned upgrade path toward some goal or target level of functionality.

C. OUTLINE OF CHAPTERS

1. Chapter II - Card System Selection Issues

This chapter discusses the important issues of card technology selection. Issues such as application attributes, security requirements, memory requirements, processing abilities, interface and interoperability, and legacy system are covered in detail.

2. Chapter III - Card Technology Overview

The history and current state of card technologies are reviewed in this chapter. It provides an introduction to each of the most common card technologies, a brief history, some common applications, capabilities, and limitations. Those items most effecting card technology selection are highlighted.

3. Chapter IV - Authentication Techniques

The current state of user and card authentication techniques is discussed in this chapter. Topics include a discussion of biometric, behavioral, and visual user identification techniques, as well as cryptographic card, and data authentication.

4. Chapter V - New Framework Background

This chapter lays the groundwork for the new framework. DoD initiatives relating to evolutionary acquisition, business process redesign, reinvention and applicable instructions, and directives are reviewed. Others concepts and theories which are used within the new framework are presented, including the analytical hierarchy process (AHP), cost estimation, risk analysis, and others.

5. Chapter VI - A Framework For Card Selection

In this chapter, a new framework for evaluating evolutionary upgrade paths for smart card systems alternatives is presented. The framework is function oriented and capability based, which is intended to be a step-by-step method that produces valuable information about the upgrade paths of selected alternatives. The steps of the framework are presented along with recommended methods and procedures for accomplishing each step. In addition, illustrative examples of the framework being applied in several different scenarios is presented.

6. Chapter VII - Conclusions And Recommendations

The summary, conclusions, and recommendations of this thesis are presented in this chapter.

II. TECHNOLOGY PERFORMANCE ISSUES

A. INTRODUCTION

Choosing the best card technology for an application can be a daunting task.¹ The number of technology options, sub-options, security options, and application alternatives can be overwhelming. Before any framework to assist with evolutionary migration to smart card technologies can be presented, an understanding of the issues involved in system performance measures is essential. This chapter provides a discussion of the major issues of card technology performance, use, and evolution. This is not an exhaustive, all inclusive discussion of possible performance measures which could be used to select a card technology, but rather some background of issues the decision maker must be familiar with and must consider before pursuing a migration to card technology systems. It will also provide the basis for the comparisons required to rate the performance of alternate technological solutions required within the new framework.

B. BACKGROUND ON CARD SYSTEM PERFORMANCE ISSUES

There have been several articles published on the selection of the right card solution for given applications. These articles have attempted to minimize the problem of card selection by centering around four or five major performance issues to be considered before selection.² While these five issues provide convenient categories to classify some

¹ Haddock, Robert, "Building the Right Card Solution into Your Application," CardTech/SecurTech '93 Conference Proceedings, 1993, p. 388.

of the major issues, there are several issues not addressed by these categories. In addition, there are many sub-issues to be discussed under each of these categories. The author contends there are eight categories of performance issues, and four additional aspects of card systems which need to be evaluated in any meaningful assessment of technologies. Each of these 12 issues will be briefly introduced here and discussed in depth within this chapter. The 12 categories are:

1. **Security Requirements** - the level of security required in the system. Security should be a function of the amount of value the card can store or contain, the classification of the data stored on the card, the value and classification of material the card system allows access to and other factors. Security has several components -- card security, authentication of user, authentication of card, and computer system security.
2. **Memory Requirements** - the type of data to be stored on the card. Memory should be a function of amount of data to be stored, how often data will be read and written, how long the data will be retained, speed of data access requirements, backup scheme, and operating system size (if required).
3. **Processing Requirements** - the logic capability (operating system) required on the card, if any. Processing requirements should be dependent on the level of complexity of the functionality desired in system, speed requirements, and the security requirements of the system.
4. **Interface Requirements** - the level of interface robustness is required. Interface requirements should be a function of the environment the card system will operate in (electromagnetic interference (EMI), line of sight (LOS), hands free, high speed, etc.), speed and amount of data transfer, and size of the card.
5. **Durability** - the durability required in a card system. Durability is composed of several components, the expected environment the card - reader interface will occur in, the cards storage environment, the reader location environment, the desired life of the card, and the life of the data stored on the card.

²Krueger, Julie, "Choosing the Right Chip For the Job," CardTech/SecurTech '94 Conference Proceedings, 1994, pp. 237-242, and Haddock, 1993, pp. 381-390.

6. **User Acceptance** - the level of user acceptance of both the card technology and any authentication techniques used. User acceptance includes privacy issues, fear of bodily damage, misuse of data concerns, and ease of use.
7. **Scalability and Expandability** - the amount to which the system can be modified or expanded in the future. Scalability and expandability should consider changes in the number of users, number of card acceptors, changes in requirements, functions, security, and memory capacity. Especially important consideration for migratory systems.
8. **Application Specific Attributes** - any attribute which is required because of the intended application.
9. **System Life Expectancy** - the useful life of the system. Life expectancy should be a function of optimal time to replace, card reader life, operation costs, and the like.
10. **Cost Estimations** - the life cycle cost of the system. Cost estimations encompass the current infrastructure, what portion of hardware, software, and data are reusable, number of card users and readers, training of users and operators, data capture, hardware, and software costs. Cost estimations also involve estimations of technology costs now and in the future, as well as economic outlook.
11. **Risk Assessment** - the technology risks involved with choosing the technology. Risk assessment consists of the age of the technology, establishment of standards, the amount of vendor support, the amount of current application, the amount of infrastructure already established, and view of the future.
12. **Temporal Component** - the value of time functionality achieved.

Each of these twelve categories is captured within the new framework. The author believes these twelve categories better reflect the full spectrum of issues which must be considered when choosing a card technology system.

C. DISCUSSION OF ISSUES

1. Security Requirements

Security within a card system, in most applications, is the most important consideration. The means of achieving security are as diverse as the types of card technologies themselves. Due to these facts, an entire chapter will be devoted to discussing authentication of cards and users. Chapter IV discusses in detail many of the aspects of security which are introduced here.

a. Level of Security Required Considerations

The level of security required in a system is a function of many factors. The most straight forward way to define the security necessary is to value what the card allows access to, and set the cost of the effort required to break security higher than this amount. Valuing the assets may be easy to do for some applications, such as a debit card systems that store a fixed dollar value. However, it is virtually impossible for other applications, such as those used to access a laboratory or computer system, or those that store highly classified data on the card. In addition to determining the adversary's cost of breaking security, it is also necessary to determine the likelihood of an attempt to break security. While the system may allow access to millions of dollars of equipment, if the desirability of access is low, there may be little likelihood of a security breach attempt, and therefore, it may be considered reasonable to take the risk associated with an attempt to break security.

The level of security chosen should be based on a clear understanding of the situation, risks, desirability, and likelihood of occurrence, and a conscious decision should be made based on these factors. The DoD supports the use of a risk analysis to determine

the security threat. A risk assessment can provide the basis for and justification of, the chosen security level.

b. Types of Security

The level of security in a card system has several major components; the security of the computer system (if used) which controls the card system, the security of the card itself, the security of the card reader, and any authentication of the user scheme employed. Security of electronic hardware such as the computers, card readers, and the data transfer between them is an issue inherent in any card system chosen. The security issues associated with electronic hardware and data transfer, as well as the security issues associated with the strength of locks, other accesses to the room, and the like will not be discussed here. The card system security issues which are dependent on the card technologies chosen, are of two main forms, authenticating the user, and authenticating the card used, and these will be discussed in detail.

Card authentication can be accomplished in a number of ways. In its simplest form, card authentication consists only of the card being the correct size, shape, and type. Many systems use this simple, inexpensive method as a screening device for access to a more advanced system. An example is an automatic teller machine (ATM), which is inside an enclosure secured by a locked door that uses a simple card authentication method to grant access to the enclosure. The ATM itself uses a more sophisticated card authentication technique, such as checking the card number against a central database.

More sophisticated techniques, that require logic capable cards, include a number of cryptographic techniques that are discussed in greater detail in Chapter IV.

Authentication of memory only, non-logic capable cards is possible as well. These memory only cards can have data stored on them using a specific encryption technique. If the data stored on the card is not in this form, the system knows the card is not authentic. The possible combinations of authentication or cryptographic techniques to card types is almost limitless. The decision maker needs to be aware of what security level the system provides, in order to properly compare alternate migratory paths.

User authentication can likewise be accomplished in a number of ways. The most common forms of user authentication today are passwords and biometrics. User authentication techniques are strongly related to user acceptance issues, and will be discussed in greater detail within that category. Both user and card authentication techniques are discussed in Chapter IV as well.

c. Error Tolerance Considerations

There are two types of errors which can be made by an authentication system, commonly called type I and type II. A type I error is the denial of an authentic user or card. These errors are also known as false rejections and are measured in terms of False Rejection Rates (FRRs). Type II errors are the authentication of a person or card which is not authentic. These errors are also known as false acceptance, and are measured in terms of False Acceptance Rates (FARs). There is a relationship between these two types of

errors. Figure 1 displays the relationship between type I and type II errors in terms of error rates (FRR or FAR) and level of assurance.

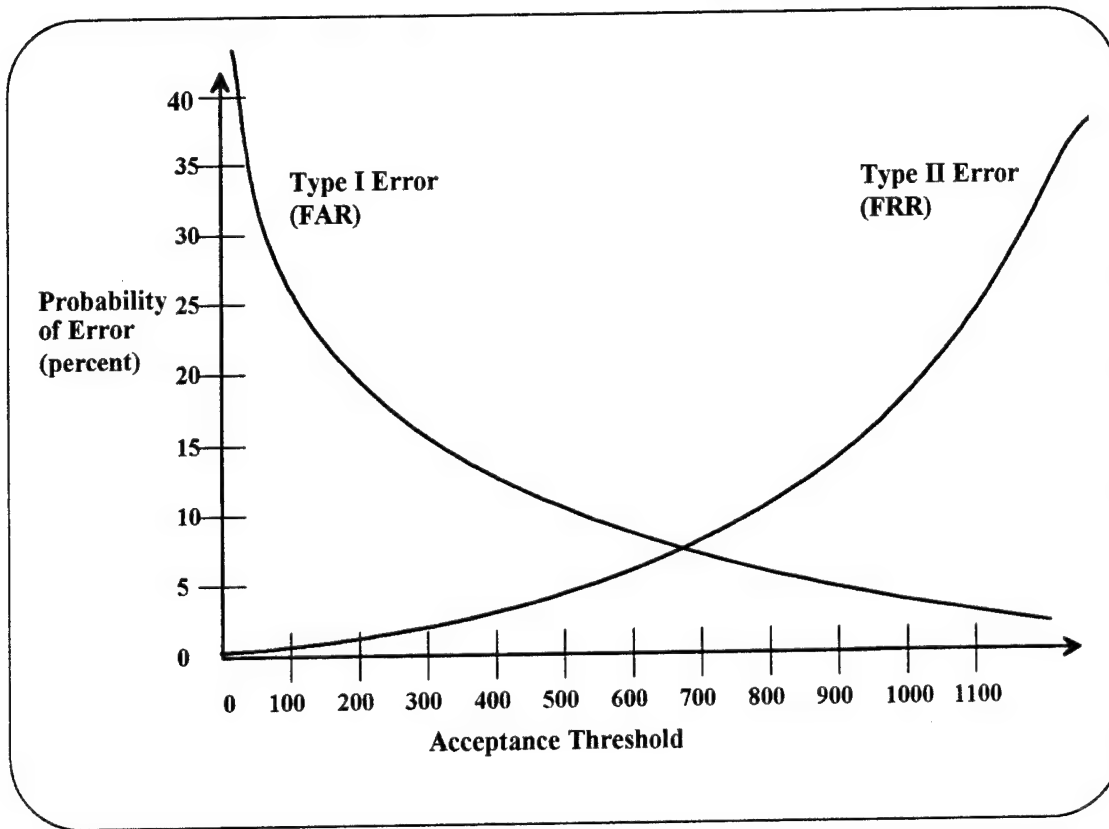


Figure 1 -- Type I Vs. Type II Errors

Each technology employed for user or card authentication, has its own set of error curves. The optimal point for the system to operate at, is a function of the technology chosen and the system designer's desires for security. If the desire is for high security with little regard for system availability, a system with low type II errors is appropriate, allowing the high type I errors to potentially make the system unavailable to authentic users. If, on the other hand, the system designer desires high system availability, with little regard for security, a system with low type I errors will be chosen, and the lower security

level will have to be accepted. In most systems, a happy medium is chosen between type I and II errors, and the authentication technique is chosen to ensure this desired level of security.

Some user authentication technologies allow for the setting of the acceptance threshold. Sophisticated user authentication techniques do not obtain the unequivocal *yes/no* answer to an authentication that card techniques do, but rather rely on a "best fit" or "close-enough" match system. This allows the level at which the system rejects users to be changed. The greater the deviance from the reference data the system allows, the higher the type II error rate will be, and the lower the type I error rate. Conversely, more stringent requirements for deviance from reference data, lowers the type II error rate, but raises the type I error rate.

2. Memory Requirements

There are three major considerations which drive the memory requirement; how much data is to be stored, the speed of data transfer required, and the characteristics of the data itself. The characteristics of the data include how often the data will be modified and how long the data needs to be retained.

a. Amount of Data to be Stored

Data capacity is the term used to define the amount of data the card technology can store. The different card technologies presented in Chapter III have vastly different abilities in the amount of data they can store. The terms and measures used for describing card data capacities are the same familiar terminology used for describing

personal computer (PC) capabilities. Memory is described in terms of bytes, and can be expressed in thousands of bytes (KB) or millions of bytes (MB). A byte is eight bits, each bit being either a 1 or a 0. The combination of eight bits represents one character. A standard single spaced page of ASCII text averages about 4 KB.³

The amount of data needed to be stored on a card is a function of several factors. A driving force is whether the system to be implemented is to be a distributed or centralized system. In a distributed system, all the data required is stored directly on the card. In a centralized system, the data is stored in a central data base. There are advantages and disadvantages to each of these schemes.

Distributed systems are being hailed as the future for the computing development agenda for this decade.⁴ They have the advantage of reducing the communications between a card reader and the central computing system, thereby making it more difficult for an adversary to capture and use these communications. Distributed systems also allow increased flexibility in the system, by not forcing all data and processing to occur in one central location. On the other hand, distributed systems require cards with substantial memory capacities, especially if the data is to be encrypted. These cards usually are more costly, slower, and less reliable. Another major disadvantage of distributing the data to card technologies, is the potential for loss of these cards. Thorough backup schemes must

³ Stanford, C.J., "What is a Smart Card," CardTech/SecurTech '93 Conference Proceedings, 1993, p. 123.

⁴ Sprague, Ralph H., Jr., and Barbara C., McNurlin, Information Systems In Practice, 3rd Ed., Prentice Hall, Englewood Cliffs, NJ, 1993, p. 167.

be developed, so the data stored on the card can be recreated in the event the card is lost. Having to maintain backup files in this manner, limits the usefulness of having a distributed system. It remains to be seen if card technology systems migrate to a distributed environment as quickly as is being suggested.

Centralized systems, in contrast, maintain all required data in a central database, and do not depend on the card technologies to store data. This allows these systems to operate on any one of the low end, less expensive card technologies. Additionally, the data is centrally managed, allowing closer supervision over access to the database. However, the security vulnerabilities associated with a central database, as well as the data transfer between the database and peripheral equipment, are considerable. A hybrid card system, where some of the data resides on the card itself and some in a central database, is also possible. This is a common configuration when a single card is to be used to access multiple systems.

For logic capable card systems, another consideration is the amount of memory storage capacity consumed by the operating system. The two major operating systems currently in use are the chip operating system (COS) and the multi-application chip operating system (MCOS).⁵ Each of these operating systems consume a substantial amount of memory themselves, thereby reducing the amount of memory available to the application. Additionally, memory space is also required to be reserved for operating system use only, in order to store intermediate results, procedure steps, data, and the like.

⁵ Stanford, "What is a Smart Card," 1993, p. 124.

b. Speed of Data Transfer

Different card technologies have different data access and transfer rates. These rates determine the amount of time it will take to transfer data between the card and the card reader. The access and transfer speed required is dependent upon the length of time that is acceptable to transfer data between the card reader and the card during a typical interaction. This length of time is referred to as the response time of the system. Response times in the half to several second range are generally considered acceptable. Faster response times make users question the error rate of the system, slower response times tend to agitate the user.⁶

c. Data Storage Characteristics

There are two major considerations of data storage; how often the data will be modified, and how long the data needs to be retained. Data items that change frequently, such as addresses or balances, can be stored in a far different manner and even on a different media, than items that do not change, such as date of birth or social security number.

There are several different ways in which data can be stored on cards. A common form of memory is write once read many (WORM) technologies. These types of cards do not allow the data to be modified. Since the data is never erased, these cards provide some security, in the form of audit trails. WORM cards do allow data to be updated. This is accomplished by writing the new data on an unused portion of memory

⁶Ondrusch, Stephan, "Smallest and Fastest Implementation of Various Asymmetric Cryptographic Algorithms on Chip Cards," CardTech/SecurTech '94 Conference Proceedings, 1994, p. 63.

and changing a pointer from the former data space to the new memory space. Since the old memory space is now tagged as unusable, WORM technologies require greater data capacities because they actually consume the memory space as data is updated. These types of memory are better for non-changing data such as medical records.

There are also *read, write many* memory types. These types allow memory spaces to be overwritten with new data. An example of this type of memory is the PC magnetic hard drive. This type does not consume memory space as updates are made, rather it writes the new data to a memory location, changes the pointer to this new data, and tags the old data memory space as available. How often the data is accessed (or read) does not effect data storage issues, but it does effect the interface requirements.

3. Processing Requirements

There are card technologies available today which possess a very capable integrated circuit chip, running sophisticated operating system, which can accomplish difficult logic operations quickly. This ability to process information significantly increases the possible applications of card technology. In the future, these cards are sure to be faster, more powerful, and have larger data storage areas. Today, however, logic capable integrated circuit cards are severely limited in usable memory area. These cards use up to about seven-eighths of their memory space for the operating system itself. This leaves only about eight KB of usable memory. Today, card system designers must choose between substantial memory space and logic ability, however this may change in the future.

Another problem with logic capable cards is the speed of memory access. If large amounts of data are to be transferred, a logic capability might not be desirable. The memory space on logic capable cards is controlled by the operating system on the card. Since these units typically operate with clock speeds of 3-5 MHz,⁷ they are considerably slower than systems which use a 33, 50, or 66 MHz card reader to access the memory space. The slower clock speed of the card chips needs to be weighed in any decisions on having processing occurring on the card itself or within the reader. The greater the level of complexity of required operations, the longer card processing will take, and the slower the response times will be. Today, complex processing should be reserved for the higher speed reader systems, and not carried out onboard the card.

The decision to use a logic capable card system also effects the security level. Logic cards are capable of more sophisticated cryptographic techniques discussed in Chapter IV. They are also generally harder to duplicate and can employ more verification and authentication techniques than other card systems.

4. Interface Requirements

The interface between the card and the card reader can be thought of as a continuous spectrum, and will be referred to in this paper as *interface robustness*. On the low end of this scale are cards which must make physical contact with the card reader. On the opposite end of the spectrum are cards capable of high data transfer rates, with the card moving at a high rate of speed at a great distance away from the reader. This type of

⁷Peyret, Patrice, "RISC-Based, Next-Generation Smart Card Microcontroller Chips," CardTech/SecurTech '94 Conference Proceedings, 1994, p. 29.

interface is not available yet, but is projected to be in the not too distant future. In between are varying combinations of distance, transfer rates and card movement speeds.

What amount of interface robustness is required in a system, is dependent on a number of factors. The first consideration should be the environment the reader-card interface will take place in. If this environment is a limiting one, such as with electromagnetic interference (EMI) or no line of sight (LOS), the interface will be required to be environment specific. The second factor to look at is any desired attributes of the application. These include hands free operation, the card or reader moving at some speed, a set desired distance for reader-card interface, or other factors.

5. Durability

The durability required in the system should take into consideration several components, such as the expected environment the reader-card interface will occur in, the card's storage environment, the environment at the reader location, and the desired life of the card and data stored on the card. The three components which make up the durability of the system as a whole are the durability of the individual components, including the reader, the card, and the interface between the two.

a. Durability of Cards and of Card Interface

The durability of the card itself is the card's resistance to damage. Most cards on the market today can stand a fair amount of abuse with out degradation in abilities. However, some cards are more durable than others. Major considerations for the cards is the environment they will be stored in. Most cards are kept in a wallet or worn on the

person. Common causes of damage to cards are magnetism, heat, flexing, bending or tearing, and scratching. Many card systems in use today replace the cards on a routine basis. This ensures the proper operation of the card when needed, and is normally not a large expense.

Different card systems use different methods of reader-card interface. The interface is frequently the limiting factor in the life of the card, especially with card systems which use a physical contact type interface. The physical contact eventually wears down the card and makes it unusable. Cards with more robust interfaces, such as ones that use radio-frequency waves to communicate with the card reader, are not so limited.

b. Durability of Card Readers and Authenticating Devices

Another factor in the overall durability of the system is the durability of hardware devices, such as cards readers and authentication input devices. These items are normally the most expensive components in the system, and are often used to determine the overall life expectancy of the card system itself. Most of these systems have mean times between failures of several years. Few require much maintenance or repair. Contact card readers may require the contact points to be replaced, but even these can last years depending on usage.

6. User Acceptance

User acceptance of the card system is an important aspect to consider. There are two main components of user acceptance; the acceptance of the card technology itself, and acceptance of any authentication technique used.

a. Acceptance of Authentication Technique

Many authentication techniques in use today are not meeting with high level of user acceptance. The problems with authentication techniques include privacy issues, fear of bodily damage, misuse of data concerns, and ease of use. Generally speaking, the more familiar the activity used to authenticate with, the more the technique is accepted. Examples of familiar activity using techniques include; voice recognition systems, signature dynamics, facial recognition, and keystroke dynamics. Less familiar activities, such as retinal and iris scans, fingerprinting, and hand vein pattern recognition enjoy lower user acceptance.

Authentication techniques which require the user to subject their person to laser or ultrasound devices, such as retinal and iris scans or hand vein patterns, suffer from fear of bodily damage. Users fear long term ill effects of the use of these devices, although there has been no data substantiating this fear as of yet.

Privacy and misuse of data fears pervade almost all authentication techniques. Misuse of data revolves more around the data to be captured when using the system, such as hours of use, time of day, number of times per week, etc., but can also involve the reference data stored to conduct the authentication. Fingerprinting is a prime example of this, stemming from its long term use for law enforcement.

b. Acceptance of Card Technology

Most card technologies are widely accepted today, and people are eager to accept new technologies. Future technologies may not enjoy this level of acceptance. The

level of acceptance is also related to the amount of infrastructure already in place and the amount of familiarization not only users but operators as well have with the technology. The importance of card technology acceptance is less than that of the authentication technique.

7. Scalability and Expandability

The scalability and expandability of the system is the systems flexibility to handle changing requirements and numbers of users. Although requirements may be well known today, they may change over the life of the system. Systems in general, and evolutionary systems especially should be designed to meet changing needs. These includes expanding functionality, number of users, and number of card readers. The determination if a systems is expandable and scaleable may be difficult to make. Although the specifications may indicate the ability to handle the larger number of users, without placing the system under such a load, it is difficult to gauge true system performance.

8. Application Specific Attributes

The category of application specific attributes is provided as a convenient category to place any other desired attribute into. What needs to be considered in this category is dependent on the specific application the system is to be used for. For example, if the system designer intends the card technology to be user as a visual identification device as well as its other functions, a card technology must be chosen which allows printing of a photograph on the card. Room for a photograph would be placed in this category and weighted along with the other factors within the new framework.

9. System Life Expectancy

System life expectancy is composed of many components. It is also a key factor in accomplishing meaningful card system evaluations. The measures of performance and costs need to be calculated for the expected life of the card system. The life expectancy can be limited by the security level in the system, the life expectancy of the hardware, or the life expectancy of the software and data. Evolutionary card systems may go through a number of software and card updates through their useful life. The cards themselves are relatively inexpensive, and card life is limited to a few years in most cases. Therefore software and cards are not good items to base the expected life of the system on. Predicting when future technological innovations will cause the security level in the system to fall below acceptable levels, is difficult, and basing life expectancy on this factor is likewise flawed. The life expectancy of major system hardware components provides a reasonable figure for overall system life expectancy. With card technology systems, the major hardware item used is the card reader or acceptor device. Since these card readers are mechanical devices, a life expectancy is a fairly easy to determine. Data on the mean time to failure (MTF) for the various card readers are available from both manufacturers and independent testing agencies.

10. Cost Estimations

As with any new technology to be acquired, cost plays an important role. In card systems, many items must go into a cost model. Card system acquisition is unique in many ways. Card systems do not have the large capital expenditures for hardware that are

associated with many other acquisitions. However, there are significant expenditures in card issuance, training both users and administrators, and in data collection. It is not this author's intent to review cost theory and analysis in this section, but rather to illustrate what research indicates are some of the major cost elements of card systems.

Card systems are also not easily compared on a cost basis. Attempting to compare cost per unit of storage for example, would be futile. Integrated circuit cards (ICCs) have only 8 KB of data storage capacity, yet can cost several dollars each. In contrast to optical cards, which can have several MB of data storage and cost slightly less. Basing a decision on the cost per byte of storage criteria alone does not capture other capabilities of the card, such as the logic capability of ICCs. Therefore, per byte storage, and many other conventional comparison schemes, are not meaningful measures. This further advances the need for an effective framework with which to compare card technology systems.

In the illustrative cost analysis presented as part of the new framework in Chapter VI, eight cost categories are identified. The cost categories are acquisition and procurement, hardware, software, data capture, operations, maintenance, training, and application specific costs. Each of these, along with some important cost considerations, will be briefly introduced in the paragraphs below.

a. Reuse of Current Infrastructure

A major factor in the cost of card technologies is the amount of reuse that will be possible in the migration path. This reuse is a consideration not only in terms of the amount of current infrastructure which will be reusable, but the amount of reuse possible

along the migration path. The migration path can be considered to have waypoints between the current and target systems. These waypoints are major milestones or major technological changes in the system. If a great deal of reusability is possible between these waypoints, overall life cycle costs will be reduced. Infrastructure reuse can come in the form of card readers, authentication devices, software, data, and the cards themselves. Backward compatibility is the term normally given to changes which allow reuse of current system infrastructure.

b. Cost Estimating

Many of the cost estimations which will be made within the new framework, are future costs, in many cases distant future. Estimating cost becomes increasingly difficult and imprecise the further one moves away from the present. The cost estimation is further complicated by the fact that many of the costs being estimated are for technology which is not even available today. The future costs also involve estimations of future economic conditions and inflation. Cost estimation concepts are discussed further in Chapter V.

c. Acquisition and Procurement

Card technology systems have similar acquisition and procurement costs to most other acquisitions. The costs involved with requirements review and system design, as well as the competitive bid process must be taken into account in any cost estimations made. These cost should not present a particular challenge to the acquisition professional, because of their similar nature to other acquisitions.

d. Hardware and Software

There are two major sources hardware cost for card technology applications, they are the cost of each individual card, and the cost of the hardware to read and interpret the card and identification measures. These are both a function of the number of each that will be in the system. Cards also have the potential of being lost; so an estimation of the number of cards expected to be lost or damaged must also be made. Most hardware items are available commercially, and cost estimation should be relatively straight forward. Installation costs of the required hardware, along with any other supporting devices such as locks, gates, wiring, etc., must also be estimated. Data supplied by vendors, contractors, and other installations having systems installed, form a basis for initial cost estimations. As discussed under cost estimating above, future cost of hardware are more difficult to estimate, and involve performing some economic as well as technological forecasting. An element of risk analysis is also involved in cost estimating, and this topic will be discussed further in risk analysis section of this chapter.

Software costs include the cost of the application software running on the central host computer, as well as any software required at the readers themselves. If logic capable cards are used, some software may be required for the card itself as well. Most of the required software should be available commercially, which would make the cost estimation relatively easy. However, it is more difficult to estimate the cost of software which must be developed or is not yet available commercially, but is expected to be

available in the future. Software cost estimation is a difficult task, and there have been numerous books, studies, and models published on this subject.⁸

e. Data Capture

Most card systems require a substantial amount of data capture during implementation. Initial data capture can consume considerable amounts of both user and operator time. Some examples of required data capture include user information database initialization, and reference authentication or biometric data capture. The amount of time, both user and operator, is an often overlooked aspect of card system setup costs.

f. Operations and Maintenance

Operations and maintenance of card systems is similar to many other electronic systems. The costs to operate the system, including manning issues, need to be figured. Card systems generally do not have high maintenance and repair costs, however, expected maintenance and repair costs need to be incorporated into the cost estimations to capture the reliability differences between alternate migration options.

g. Training

Any time a new technology is adopted by an organization, training is required. This training needs to be not only for the operators of the system but for the users of the system as well. The amount of time and effort required to conduct the training depends on several factors. The education level of the user, difficulty level of user operation, familiarity of operators with the this or similar technologies, difficulty level of operation,

⁸Boehm, Barry, Software Engineering Economics, Prentice Hall, Englewood Cliffs, NJ, 1981.

and other similar factors should be taken into account when performing these estimations. Additionally, some training on the need and basis for the change may be appropriate to ensure the users are receptive to the change and accept the new technology.

h. Application Specific Costs

The category of application specific costs is provided as a convenient place to put any other anticipated application specific costs. What costs need to be considered in this category is dependent on the specific application the system is to be used for. An example would be the potential scrap value of components as system migration occurs.

11. Risk Assessment

The term *risk assessment* can take on several meanings depending upon the context in which it is used. Earlier, in the security section of this chapter, security risk assessment was discussed. Security risk assessment involves estimating the likelihood, or assessing the risk of, a security breach. In the cost estimation section, an economic risk assessment was made, in the form of estimating future costs, future economic conditions, and the likelihood of each. In this section, risk assessment refers to the assessment of technological risks. Many assumptions of the future state of card technologies will have to be made to develop the various migration paths toward a target system. Each of these paths will have a likelihood of occurrence and an amount of risk to project failure associated with it.

Some factors which should be considered when assessing the technological risks are the age of the technology, whether or not standards have been established, how great

the disparity between current technology and assumed technology is, and the desirability of assumed technology for example.

12. Temporal Component

With migratory system comparisons, different migration paths will produce different functionality at different points in time. The value of this temporal component must be assessed in any meaningful comparisons of migration paths. Capturing this comparison is not easy. Within the new framework, this time preference is captured by a simple time preference weighting scheme. However, the weighting scheme is for all functionality, and not for each individual measure of performance. Weighting the time preference for each individual measure of performance is possible, however, it complicates the calculations considerably. The information gained from using this type of a time preference scheme would be marginal, and given the inaccuracies inherent in any estimation method, the result would provide little benefit.

D. CONCLUSION

There are many aspects of performance issues which need to be captured in any decision of card technology application. This chapter introduced many of these issues and some of the considerations which should go into making these decisions. This chapter also discussed how many of the steps within the new framework address these factors which must go into card technology selection.

III. CARD TECHNOLOGY OVERVIEW

A. INTRODUCTION

Before a framework for evolutionary migration can be presented, an understanding of the current state of card and card compatible technologies is required. This chapter provides background on the different card technologies currently being applied. For each different category of card technology, this chapter provides a short history, a system description, capabilities, limitations, and some common applications. Card technology is an extensive topic, with far more information about card technologies and their applications than is presented here. The user of this thesis need not be concerned with all the nuances of this technology, but rather needs a firm understanding of the base technologies and how they can be applied. This chapter provides the foundation needed to understand and apply a card technology selection methodology, however, it is not intended to be an exhaustive discussion of the topic.

B. HISTORY OF CARD EVOLUTION

The term *card technology* encompasses a wide assortment of different systems. The broad definition includes any technology that will fit on an industry standard card. The International Standards Organization (ISO) Standard 7810 defines the dimensions of an industry standard card to be 85.6 (± 0.12) millimeters (mm) by 53.98 (± 0.05) mm and

0.81 (\pm 0.01) mm thick.^{1,2} The card medium, although normally a plastic, can be cardboard, paper, pasteboard, or a variety of other materials.³

Over 40 years ago, *charge-a-plates* became popular. These were metal plates which were issued by retailer-owned association for the purpose of extending credit to customers. The plates were embossed with the customer's name and account number.⁴ The evolution of cards, into the form we know them today, began in the 1960s with the invention of Polyvinyl Chloride (PVC) and Polyvinyl Chloride Acetate (PVCA). The advent of this material made it possible to produce small, durable, flexible, embossed cards. PVC is still used in many card applications, however, it is not the only material in use. PVC is not recyclable and cannot be injection molded. Injection molding is the formation of a card by pouring (or injecting) a liquid material into a mold. PVC cards must be cut from sheets of PVC and machined to make the recess for the chip, costing considerably more.⁵ Recent attention to environmental concerns and economic costs, cause PVC to be less and less desirable. There have been many advances in material sciences in recent years, including the invention of Acrylonitrile Butadiene Styrene (ABS), which, although not embossable,

¹ This is approximately 2.125" x 3.375" x 0.030" thick.

² With the exception of PCMCIA cards which will be discussed in more depth later.

³ Svigals, Jerome, Smart Cards: The new Bank Cards, MacMillan Publishing, NY, NY, 1987, p. 195.

⁴ Linden, Larry F., "Introduction to Card Technology and Biometric Workshop," CardTech/SecurTech '93 Conference Proceedings, 1993, pp. 3-6.

⁵ "The Chip Card: A New Data Carrier Made of Plastic," Smart Card Technology International, 1994, p. 50.

is recyclable and can be injection molded. ABS is becoming the preferred medium for chip cards while PVC remains the preferred medium for magnetic stripe cards.⁶

The next major event in the evolution of card technologies, was the card stripe standard, set by the American National Standards Committee (ANSC) in 1973. This standard was the first step in wide spread standardization and acceptance of a card technology. It defined machine readability standards, physical characteristics, data density, location of embossing, magnetic recording techniques, and the like. In 1980, the VISA / Master Card consortium published the Bankcard Stripe mandate. This mandate required businesses to have the required magnetic stripe infrastructure by 1983, if they were going to accept VISA / Master Card. This mandate eventually led to widespread acceptance of magnetic stripe technology and the proliferation of magnetic stripe infrastructure.⁷

Integrated circuit card (ICC) history begins with the patents for ICCs, which were first granted in 1970. However, there were no large scale applications of ICCs until 1985, when France Telecom selected smart cards over magnetic and holographic cards as the medium for payment on public telephones.⁸ The French government sunk millions of francs into the development of ICCs in the early 1980's.⁹ This extensive use of smart

⁶ GemPlus, Welcome to Smart Cards, draft copy, 1993, p. 21 and "The Chip Card...", 1994, p. 50.

⁷ Linden, 1994, p. 6.

⁸ GemPlus, 1993, p. 4.

⁹ "Smart Card Draws a Blank," New Scientist, Vol. 99, No. 1371, August 18, 1983, p. 456.

cards by the French, in such a common application as public phones, lead to the rapid acceptance of smart cards in France and the rest of Europe. The patent for contactless ICCs was granted in 1973, only three years after the contact ICC patent. However, it suffered from lack of application until the mid-1980s as well. Contactless technology has been employed extensively in radio frequency identification (RF/ID) applications for many years. Radio frequency identification applications normally employ small electronic tags which are attached to items that are to be tracked. These tags respond with their identification when interrogated by the system. Contactless ICCs are the transformation of this technology onto industry standard cards.

The introduction of the optical card in the early 1980s was another major event in the evolution of card technologies. However, only recently has optical card technology evolved to the point of providing a viable technology at reasonable cost. Standards for optical cards are still being written by the International Standards Organization (ISO) and are expected to be finalized by 1995. As has been seen with other card technologies, completion of the standards should be a major boost for this technology.

The latest evolution in card technologies is the Personal Computer Memory Card International Association (PCMCIA) issuance of the Personal Computer Memory Card Interface Adapter (PCMCIA) standards in the early 1990s. PCMCIA cards are thicker and more capable than other card technologies. The infrastructure proliferation for these cards has experienced an explosion since the issue of the standards, fueled largely by the

popularity of devices such as laser printers, notebook computer systems, palmtop computers, personal digital assistants, and the like.

C. CARD TECHNOLOGIES

This section describes each of the machine readable card technologies. Machine readable card technologies are loosely defined as any system which fits on the industry standard card and can "communicate" or be read by a computer or other reading device.

1. Bar Codes

a. History

Bar coding did not start as a card technology and current major applications are not on cards. However, bar codes have been successfully used in a variety of card applications. Bar codes are machine readable, however, they do not truly "communicate" with a reader, rather they provide the reader with a single line of data of varying size, dependent on the type of bar code. The reader must store all the required data about the item in a central database.

Bar codes were initially driven by retail applications and have been in extensive use since the Universal Product Code (UPC) was accepted as the industry standard on April 3, 1973. Although bar codes were originally developed for point of sale (POS) applications, they quickly spread to other uses, including industrial applications, and card technologies.

b. Systems Descriptions

Bar codes are patterns of parallel bars and spaces of varying widths that represent characters. The spacing of the bars and spaces is called a symbology. There are many symbologies in use today, the more common ones are briefly discussed below.

There are two major categories of bar code symbologies; discrete and continuous. Discrete symbologies allow the characters to stand alone and be decoded independently from other characters. The characters are separated by spaces. Continuous symbologies have no spaces between characters; the end of one character is the start of the next. Continuous codes with multiple element widths are the most common and most capable codes. These codes are referred to by their (n,k) designation, "n" being the width of the character (n modules) and "k" being the number of bars and spaces. The total number of possible patterns in each element of a (n,k) symbology scheme is given by Equation (1)¹⁰.

$$(n - 1)! / [(2k - 1)! \times (n - 2k)!] \quad (1)$$

For example, the standard UPC symbol is a (7,2) symbology, which allows a total of 20 possible different patterns as shown in Equation (2).

$$\begin{aligned} & (7-1)! / [(2 \times 2 - 1)! \times (7 - 2 \times 2)!] & (2) \\ & = 6! / (3! \times 3!) \\ & = 720 / 36 \\ & = 20 \end{aligned}$$

¹⁰Palmer, Roger C., The Bar Code Book: Reading, Printing, and Specification of Bar Code Symbols, 2nd ed., Helmers Publishing, Peterborough, NH, 1991, p. 19.

With 20 possible patterns in each of the 10 digits of the code, the total number of possible different UPC codes is $20^{10} = 10,240,000,000,000$. The most capable bar codes can store up to 40 characters of data, with considerably more than 20 combinations per character, giving them an even greater number of possible combinations.

Bar codes are read by a beam of light scanning the bar code. Dark bars absorb the light and spaces reflect the light back to the scanner. The scanner transforms the light reflections into electrical impulses which can be decoded into characters. Scanners can use a variety of light sources, including lasers, visual Light Emitting Diodes (LED), and infrared LED. Current technology allows scanners to read anywhere from direct contact to several feet away.¹¹

(1) Code 39 Bar Codes. Code 39 was the first alphanumeric symbology developed and is still very popular in industrial and government applications. It is a discrete code, using two different widths of bars (a two-width code). There are 44 characters in code 39's character set, each consisting of five bars and four spaces, three of which are wide and six of which are narrow. Code 39 is also known as "3 of 9 code", from the 3 wide bars of 9 total bars. Code 39 can be used to encode the entire 128 character set by using two sets of nine bars and spaces to represent each character. Using this symbology, it is possible to produce codes of any practical length to meet varying needs. Code 93 is very similar to code 39, however, it is a continuous code (9,3) and is used to complement code 39. An example of a Code 39 bar code is given in Figure 2.

¹¹ Palmer, 1991, p. 70.



Figure 2 -- Code 39 Bar Code¹²

(2) Code 128 Bar Codes. Code 128 was introduced in 1981 and is an alphanumeric symbology of 106 different characters. It uses blocks of three bars and three spaces, all of which fit into 11 modules (11,3). There are four element widths, and elements can be of from 1 to 4 modules wide. It also uses a check digit to perform a simple check sum on the code to ensure it was read correctly. Figure 3 is a sample of a code 128 bar code.

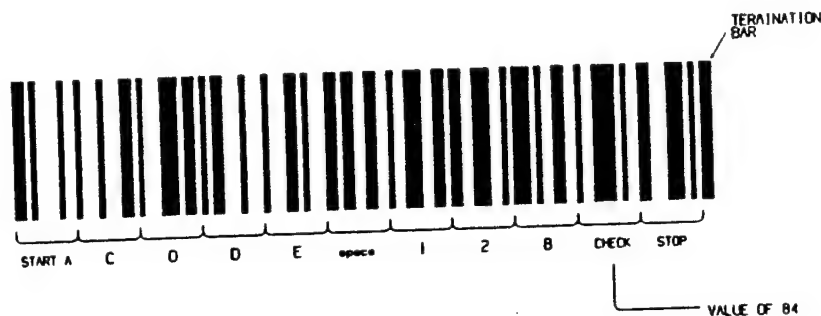


Figure 3 -- Code 128 Bar Code¹³

¹²Palmer, 1991, p. 33.

¹³Palmer, 1991, p. 37.

(3) Universal Product Codes (UPC). As discussed earlier, UPC codes originated in the early 1970s. The most common form, Version A, is a fixed length code symbology, employing a 12 digit code. The first digit is a number system digit, indicating whether the item is a coupon, a product, an in-store marking, or other category. The next ten digits are broken up between the manufacturer (five digits) and the product (five digits). The final digit is a check sum of the proceeding 11 digits. UPC symbology uses two spaces and two bars varying from one to four elements long for each symbol (7,2). Versions B, C and D are not commonly used. Version E is used for small products and incorporates only 6 digits. Europe uses a superset of UPC, known as the European Article Numbering (EAN) system. An EAN scanner can decode UPCs, but the inverse is not possible.¹⁴ Figure 4 gives an illustration of a standard UPC.



Figure 4 -- Universal Product Code Bar Code

(4) Interleaved 2 of 5. Interleaved 2 of 5 is a self checking, continuous numeric symbology that is widely used in the distribution industry. Every character

¹⁴Palmer, 1991, p. 24.

encodes two digits, one in the bars and one in the spaces. This symbology consists of five bars and five spaces in each character, two of the bars and two of the spaces being wide and three of the bars and spaces being narrow. This sequence of bars and spaces provides 100 unique symbols. It can be used in varying lengths and can incorporate check sums and the like. Figure 5 provides a sample of a interleaved 2 of 5 bar code.



Figure 5 -- Interleaved 2 of 5 Bar Code¹⁵

(5) Code 49. Code 49 was introduced late in 1987 as a symbology for labeling small items. It consists of two to eight adjacent rows, separated by a one module bar. This symbology is a (16,4). Figure 6 provides a sample of code 49 bar coding.

(6) Code 16K. Code 16K symbology is similar to Code 49, but 16 rows of symbols may be used. This symbology uses standard Code 128 (11,3) character patterns without individual row check characters, however, there are two overall check characters. Each row is 70 modules long and encodes five data characters. Since this symbology allows a variable number of rows, a single character at the beginning is used to indicate total number of rows.

¹⁵ Palmer, 1991, p. 27.

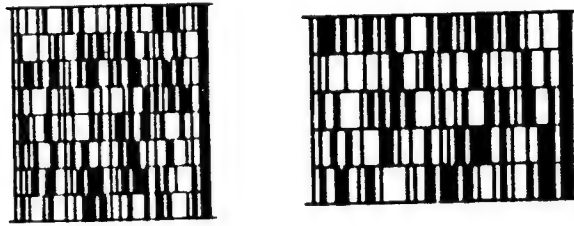


Figure 6 -- Code 49 Bar Codes¹⁶

(7) Other Symbologies. The above mentioned symbologies are established industry standards and have well established vendor networks.¹⁷ There are, however, countless other symbologies currently in use in specific applications. These include PDF417 (17,4), 2 of 5, Codabar, Codablock, Code 11, Plessey Code, Postnet, and a large number of even lesser known symbologies. While the reader need not be concerned with the variations of all of these, it is beneficial to know that there are many out there, one of which may be able to fill a specific requirement.

c. Common Applications

Bar codes are normally used in centralized database applications, where there is a need to quickly and accurately capture a high volume of items. Each item is assigned a unique bar code and the central database maintains all the data about the item. The most common applications for this technology is in retail stores at the point of sale (POS), libraries, inventory, and manufacturing tracking and control. When applied to card

¹⁶Palmer, 1991, p. 42.

¹⁷Palmer, 1991, p. 47.

technologies, it is used to record single lines of non-changing data such as account numbers, name, social security number, etc., to allow rapid, error-free capture and recording of these data fields.

d. Capabilities

Bar coding is an inexpensive technology that allows rapid capture of a fairly complex string of alphanumeric characters. Bar codes can be printed on adhesive strips using a laser printer and software, resulting in bar codes for fractions of a cent each. Bar code readers are also are inexpensive, typically less than \$100 each. There are well established standards and a wide variety of vendors. This relatively simple technology does not require advanced expert knowledge for installation or maintenance.¹⁸

e. Limitations

The 40 character limit on data in a bar code does not support distributed data, rather it requires an extensive database to store all the required data about the codes. This normally requires a healthy investment in manual data entry somewhere in the process. Bar codes provide no security; they can be easily duplicated or counterfeited by anyone with bar code printing software. Bar codes cannot be modified, but must be reprinted to update. Additionally, they are easily damaged by scratching, rubbing, dirt, fog, and mist.

¹⁸ Information Spectrum, Inc., brochure, February 16, 1994, pp. 23-24.

2. Magnetic Stripe Cards

a. History

Magnetic stripe technology began in the late 1960s. Magnetic stripe technology is the most widely used card technology currently on the market, with several billion cards of various forms in use today¹⁹ and about 1.3 billion cards being produced every year.²⁰ The majority of these are financial transaction card (FTC) applications, (more commonly known as credit cards) and Automatic Teller Machine (ATM) cards.

Magnetic stripe cards began in response to a need for the automatic recording of account numbers. Embossed credit cards, with the account number and name in raised lettering on the card, flourished from 1950-1970. Because of this, the account numbers grew in length. These longer account numbers lead to difficulty in accurately recording them and a high error rate. Larger account numbers required automatic capture, hence the development of magnetic stripe cards.²¹

b. System Description

Standard magnetic stripe cards have a single 0.5 inch wide, 0.0005 inch thick band of magnetic media that runs the entire length of the card. The media lies 0.223 inches from one of the long edges of the card. These magnetic stripes are typically thought to be across the top back of the card, although the card may be printed with any

¹⁹ Svigals, 1987, p. 21.

²⁰ Lavelle, Francis, "The Smart Card," Smart Card Technology International, 1994, p. 42.

²¹ Svigals, 1987, pp. 20-38

orientation. All other area on the card is free for additional media, printing, raised lettering, etc.

The volatility of data stored on a magnetic stripe is dependent on the type of magnetic medium used. There are several magnetic media in use, which fall into two categories: High coercivity (HiCo) and Low coercivity (LoCo). Coercivity is the amount of energy that is required to change the magnetic state of the material and is measured in oersteds.²² Barium Ferrite (BaFe) is the most common HiCo material and Iron Oxide (Fe_2O_3) is the most common LoCo.²³ The higher the coercivity of the material used for the magnetic stripe, the less chance there is for accidental erasure and altering. However, it is more difficult to initially record data on HiCo material, which results in increased cost of writing to the cards.²⁴

This magnetic medium is comprised of three tracks, each 0.110 inches wide. Track one has a recording density of 210 bit per inch (bpi) and can hold 79 alphanumeric characters and is normally used to hold data pertaining to the card holder. Track two is 75 bpi and holds 40 numeric characters. It is designed to hold information for the automation of financial transactions, such as account number, expiration, type, etc. Track three is

²² Dreifus, Henry, "Public Telephone Applications for Card Technologies; Practical Applications, Issues and Future Trends," CardTech '92 Conference Proceedings, 1992, pp. 3-6.

²³ Kutchera, Arthur, "High Coercivity Media," CardTech '92 Conference Proceedings, 1992, p. 36.

²⁴ Mos, Robert, "High Coercivity Encoding," CardTech '92 Conference Proceedings, 1992, p. 57.

again 210 bpi and can hold 107 numeric characters. This track is intended for information that will be updated with each transaction, such as balance.²⁵ Many magnetic stripe card applications do not utilize all three tracks, even though all three are printed on the cards. Recently, cards have begun appearing with 0.33 inch magnetic strips, containing only two tracks, as the frequent updating of magnetic stripes is not common.

To read from or write to a magnetic stripe card, the card must be moved under a recording or reading head. A recording head receives the encoded data (1s and 0s) and records it on the magnetic material by reversing the magnetic flux of the material in the magnetic stripe. A reading head detects flux reversals in the magnetic stripe, and a decoder translates these to data. Magnetic stripe cards are most commonly read by inserting the card into the reader or by passing the card through (called a swipe, from the hand motion of moving the card through the reader). Figure 7 provides a typical layout of a magnetic stripe card.

c. Common Applications

The dominant use of magnetic stripe technology continues to be financial transaction card (FTC) applications, such as credit cards, automatic teller machine (ATM) cards, and bank cards. Because of the inexpensive nature of LoCo magnetic material, narrow, single tracks are frequently applied to disposable cards. These are used for fare collection in metro systems, amusement park rides, telephone calls, and the like. There

²⁵ Svigals, 1987, pp. 25-26.

are several other applications in place as well, from inventory tracking, to access control, to time and attendance accountability.

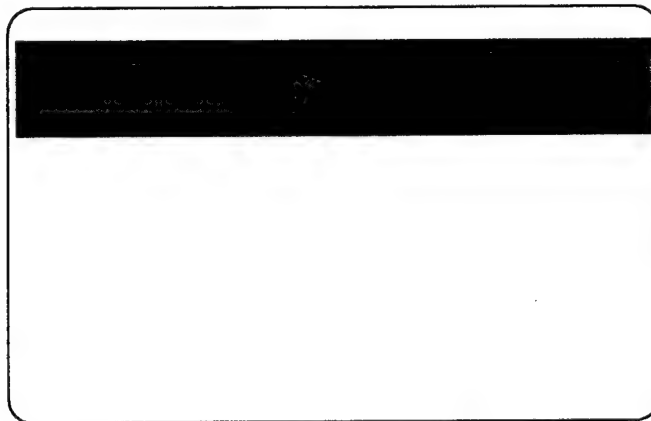


Figure 7 -- Magnetic Stripe Card

d. Capabilities

Magnetic stripe card technology has been in use for over two decades. The standards are well established and the technology has significant vendor support. The infrastructure, at least for credit card applications, is in place throughout the world. Due to its popularity, standard magnetic stripe cards and readers are inexpensive. This low cost, both of cards - (typically under \$0.50 each) and of readers/writers (readers: about \$25.00 each; writers: about \$500.00 each),²⁶ is magnetic stripe technology's major attraction.

e. Limitations

Magnetic stripe cards have many limitations. They provide little security. Magnetic stripes are easily read, altered, erased, copied, or counterfeited. LoCo cards

²⁶ Stanford, "What is a Smart Card," 1993, p. 121.

are easily damaged or destroyed by demagnetizing. HiCo cards, while less easily damaged, are still susceptible to demagnetization. They are also easily damaged by scratching, bending, dirt, etc. The life expectancy of a magnetic stripe card is only a few years, causing the need for reissue on a routine basis.

Magnetic stripe cards are very limited in their data storage capacity of between 150 and 475 characters.²⁷ In most applications, this limited data capacity requires the use of a central database to store other required data. They are not well suited for decentralized database use.

3. WIEGAND CARD TECHNOLOGY

a. History

Wiegand technology was introduced into the market in 1979. It was invented by John Wiegand, and the patents are held by Echlin Incorporated. When it was introduced, it was the first completely new card technology to be placed on the market in over a decade.²⁸ There is a large installed base of Wiegand technology access control applications, due to its relatively low cost, high capability and 25 years of use.

b. System Description

Wiegand cards consist of from one to 56 wires laminated within the plastic of the card. Each of these wires can represent a bit of data, and can take on one of a number of values. This allows an almost limitless combination of individual codes. The codes are

²⁷ Information Spectrum, Inc., 1994, p. 22.

²⁸ Mourey, Richard, "Wiegand Card Technology Remains A Secure Investment," Security Technology and Design, Vol. 4, No. 6, August 1994, pp. 42-44.

produced by giving ferromagnetic wires unique magnetic properties. The wires are thin (0.10 inches) and are composed of two dissimilar materials, an outer shell and an inner core. The shell is heat treated and hardened, giving it set magnetic properties. The core is a soft material with changeable magnetic properties. When the wire is subject to a strong magnetic field, both core and shell have magnetic north at the same end, and the wire possesses its own magnetic field. If the wire is subjected to weaker magnetic fields oriented in the opposite direction, the core material may switch polarity, depending on the strength of the weaker field. If the core material does switch polarity, it causes the wire's external field to collapse. These collapsing and returning magnetic fields from the wire can be sensed by coils placed near the wires (i.e. in the reading device), and translated into discrete analog electrical impulses. The pulses are crisp enough to be read as digital outputs. The electrical impulses are produced without using electrical input, requiring only relative motion between the wires and the magnetic fields of the reading device.²⁹ These systems normally use motion of the card through the reader to produce these electrical impulses, vice having the magnets in the reader move.

c. Common Applications

Wiegand technology's most common application is in access devices. The systems simplicity, durability and limited maintenance requirement make it well suited for access devices in hostile or remote applications. This technology has had little application outside this field. Although it is possible to use Wiegand card systems as an automated

²⁹ Mourey, 1994, pp. 43-44.

data capture device, similar to how magnetic stripe cards are often used, this is not a common application. Wiegand card systems cost more and have less data capacity than magnetic stripe cards. However, Wiegand cards provide greater security against duplication, security which is not warranted in most automated data capture applications.

d. Capabilities

Wiegand technology cards provide significant advantage in card and reader life expectancy and durability. Since the cards contain only separate wires, there are no electronic circuits, soldered connections, or contact points to wear out or break. These wires are laminated within the card, providing protection from damage. The readers are likewise very durable, since there is no requirement for moving or electrical parts.

The Wiegand cards themselves rank fairly well in security. They are difficult to copy, duplicate, or counterfeit. Tampering with the card destroys the wires and magnetic properties. However, these cards do not support any form of cryptography, biometrics, or any other advanced authentication schemes. The card faces are available for printing, photographic imaging or other visual authentication methods. This technology could be used with other technologies on a hybrid card.

e. Limitations

Wiegand cards are not able to be changed (or programmed) by system administrators in the field. They must be manufactured with their codes. This requires system designers to rely on the same vendor for all the cards which will be needed throughout the useful life of the card system. Wiegand systems also do not expand or change easily. Not

being able to program cards presents a significant inconvenience. The lack of ability to support user authentication security also limits their usefulness in advanced, automated access control systems.

4. INTEGRATED CIRCUIT CARDS

a. Background

Integrated Circuit Cards (ICCs) are available in a variety of types, each of which is described below. There are two major distinctions for ICCs: Whether they are contact or contactless cards; and whether they have a logic capability or are memory-only. These two major distinctions provide four of the categories of ICCs described below. Super smart cards are an extension of contact smart cards, having an input/output (I/O) method. The final category, Personal Computer Memory Card Interface Adapter (PCMCIA) cards, are thicker than standard cards and may contain multiple integrated circuits (ICs).

Much of the terminology that is used to describe these relatively new technologies is not firmly set yet -- especially the term "*Smart Card*". The term smart card is often loosely applied to any card which has an integrated microchip. However, as already discussed, these fall into two categories; memory-only chip cards (that have no on-board processor and therefore no logic ability) and micro-processor chip cards.³⁰ The former "cannot manipulate data and therefore do not deserve the attribute of smartness."³¹ For

³⁰ Bass, Peter, "Cards in Communication," Smart Card Technology International, 1994, p. 32.

³¹ Stanford, "What is a Smart Card," 1993, p. 117.

the purpose of this paper, the term "*programmable IC card*" will be reserved for logic capable (micro-processor chip) cards, whether contact or contactless. The term *Integrated Circuit Card (ICC)*, in accordance with the International Standards Organization (ISO), will be used for the broad category of all integrated circuit cards. The term "*memory IC card*" will be used for non-logic capable, memory-only ICCs. This is generally in accordance with industry norms, however, the reader may be exposed to other terms for ICCs, such as microcircuit cards (an International Association For Microcircuit Card's (INTAMIC) designation for ICCs), chip card (referring to the common name for ICs), and the term smart card applied loosely to all ICCs. Figure 8 provides the names commonly used for different technologies and the relationships between the technologies. The terms used in this paper are indicated by bold type; other names commonly encountered are italicized.

The reader may also encounter IC chips in a variety of different media, such as in a plastic case in the shape of a key³² or a dog tag (data tag).³³ These applications, although not true card applications, resemble the ICCs in many ways. The contact points for the ICs are in a different place than on a card, but functionality is normally quite similar. Alternate types of media often provide a higher level of protection for the IC than a thin card does. These applications are far less common than ICC, because they do not

³² Such as is used in STU-III telephone systems for example.

³³ Svigals, 1987, pp. 40-41.

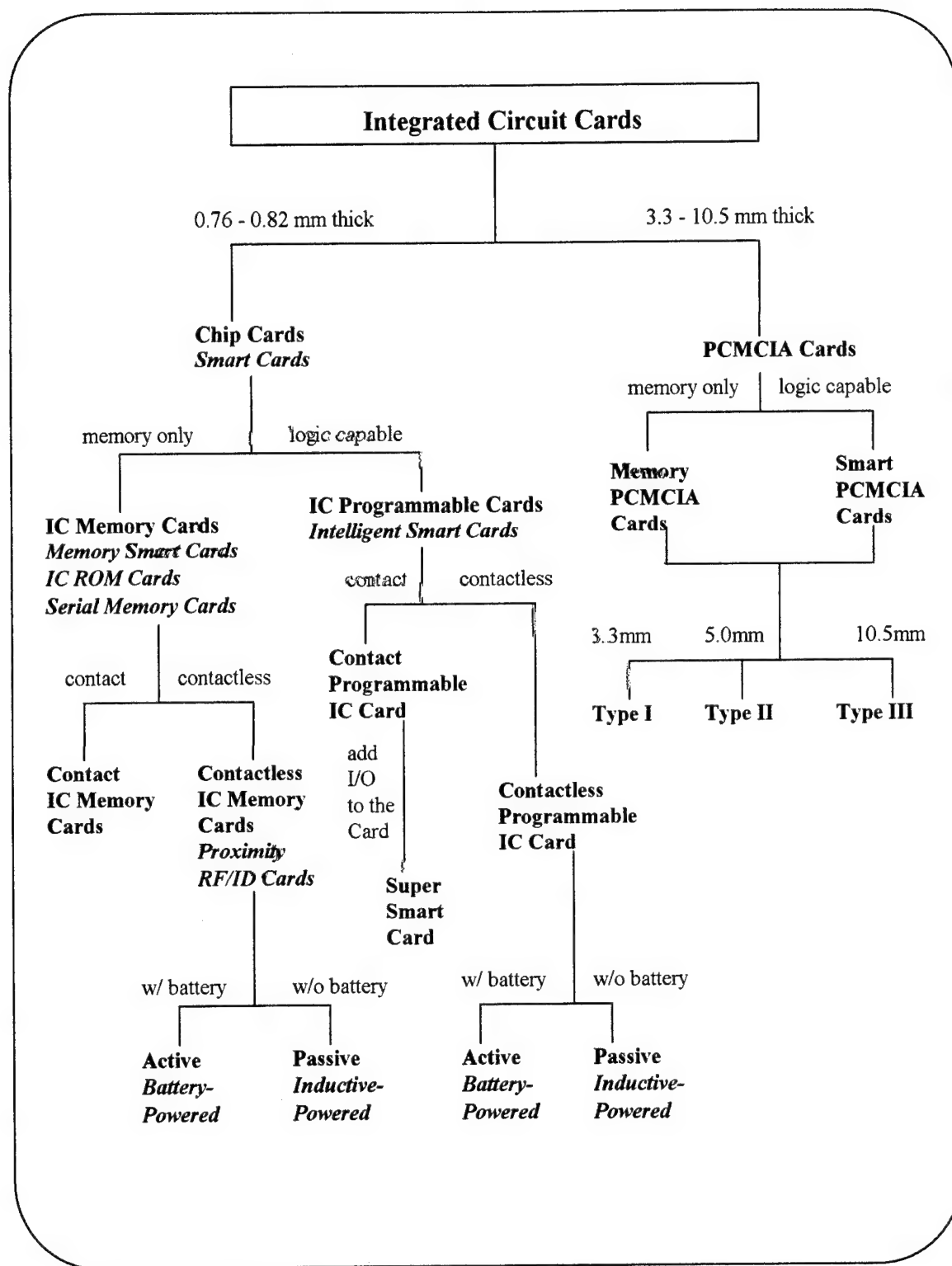


Figure 8 -- ICC Technologies Hierarchy

conform to the current in-place infrastructure, the standards are not well defined, and therefore, they can only be used in their specific application.

b. Evolution of the IC Card

In the early 1970s, with the emergence of integrated circuit chips sufficiently small enough to fit on a card, smart cards were introduced by Motorola.³⁴ However, these cards did not gain popularity until the mid 1980s. The first large scale application of ICC cards was in 1985, when France Telecom selected smart cards over magnetic and holographic cards as the medium to use for payment on public telephones.³⁵ Smart cards provided much greater security against fraud than the other card technologies. Smart card use for public phones followed in many other European and Asian countries.

Around 1970, ICs became small and flexible enough to allow them to be placed on cards. Integrated circuits, microscopic electronic circuits etched onto semiconductor substrate, are more commonly known as "chips." These first chips were not capable enough to warrant the large scale investment required to develop ICC applications. With the advances made during the late 1970s in chip design, more and more capable ICCs began appearing. The early 1980s saw the first implementations in ICC systems. A Frenchman, Roland Moreno, is credited with inventing ICCs in 1974. However, Kunitakda Arimura, who is Japanese, obtained patents for contact ICCs in 1970, and

³⁴ "The Chip Card...", 1994, p. 50.

³⁵ GemPlus, 1993, p. 4.

contactless ICCs in 1974.³⁶ Credit is generally given to the French for having been the first to implement ICCs on a large scale. In 1985, France Telecom decided to use ICC technology in its public phones. By 1992, over 60% of France's public phones used smart cards.³⁷

ICCs use an integrated circuit of 25 mm square. This size limitation standard was set after extensive testing demonstrated this to be the optimal size. It is the largest area which allows the flexibility required to have a reliable card. Using a chip larger than 25 mm² causes the ICC to have a high failure rate under to the expected stresses cards receive. Chips smaller than 25 mm² severely degrade the capability of the IC and produce a marginal gain in reliability.

As of early 1994, there had been 50 million integrated circuit chips supplied for smart card applications.³⁸ Although this is a far cry from the 1.3 billion magnetic stripe cards issued each year, it is predicted there will be an explosion of smart card applications in the coming years, with 575 million smart cards in use by 1996³⁹ and one billion in use by 1998.⁴⁰

³⁶ Won, Duk, J., "Introduction to Integrated Circuit (Smart) Cards," program management review paper, February 26, 1991, p. 4.

³⁷ GemPlus, 1993, p. 4.

³⁸ "The Chip Card...", 1994, p. 50.

³⁹ Seidman, Stephan, "Advanced Card Technologies," CardTech/SecurTech '93 Conference Proceedings, 1993, p. 24.

⁴⁰ GemPlus, 1993, p. 21.

c. Contact Chip Cards

(1) System Description. Contact chip cards use a single IC (or chip) placed in a recessed area which has either been milled in or stamped on to the card. The chip has contact points which make point-to-point contact with the reader/writer device in order to communicate. Although chip configuration, design, and appearance vary among manufacturers, the contact points are always in the same place to ensure compatibility. The IC is powered, through the appropriate contacts, from an interfacing device, commonly known as card acceptor device (CAD), . Data and logic information likewise flow through a set of contact points. Figure 9 provides a typical layout of a contact chip card.

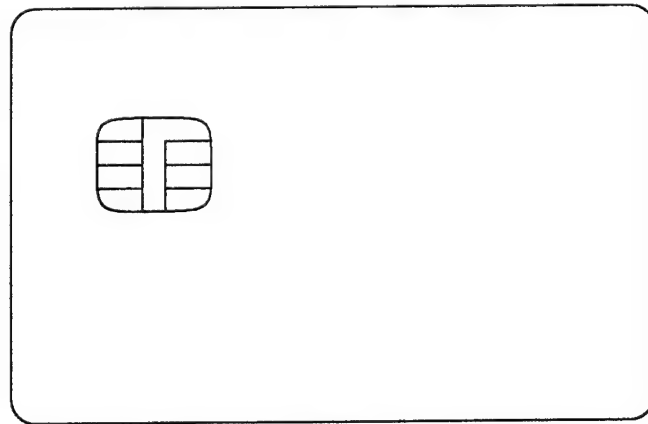


Figure 9 -- Contact Chip Card

(2) IC Programmable Cards. The programmable IC chip has logic capabilities, which allow it to carry out specific functions, respond to the external commands of the interfacing device, perform calculations, access memory, carry out a set of instructions, and make a host of other logic decisions and responses.⁴¹ In order to carry out these

⁴¹ Svigals, 1987, p. 39.

functions, these cards must be programmable, and therefore need an operating system (OS). There are two operating systems available for IC programmable cards, the chip operating system (COS) and the multi-application chip operating system (MCOS), the latter providing more capability.⁴² These operating systems allow the IC to operate like a computer on a card. The ICs for these cards operate on 8-bit microcontroller architecture. The clock speeds are determined by the power being supplied to the card's terminals from the interfacing device and are typically 3-5 MHz.⁴³

(a) Common Applications. Contact programmable IC cards are being used in an ever increasing array of applications. They are an extremely capable card technology, combining a logic ability with a memory space. Their potential applications are limited only by the imagination of the system designer. Some of the major categories of use are discussed in the following paragraphs.

Their use as a financial transaction card (FTC) is steadily increasing, especially as the price per card decreases and the infrastructure grows. While they have been slow to catch on in the United States, their use in Europe has blossomed, with the payment of public phone charges being a driving use. Credit card applications have been comfortable with the magnetic stripe technology, but with the vastly superior capabilities of the contact IC card and increasing security threats, that may change in the near future.

⁴² Stanford, "What is a Smart Card," 1993, p. 124.

⁴³ Peyret, 1994, pp. 9-36.

Another expanding use for these cards is the electronic delivery of benefits such as food stamps, aid for families with dependent children, and other benefit payments. This is commonly called Electronic Benefit Transfer (EBT). Because of the security capabilities and memory space, they can be initialized with a value, decremented as they are used, then "recharged" with value again when the person is eligible. Using a card technology in this fashion would provide significant savings in the printing, collection, administration, and destruction costs of the current paper system. Through the use of biometric identification,⁴⁴ it would also provide a better guard against fraud (multiple claims by the same individual) in the system. Many states and the federal government are looking into this technology as the future for EBT.⁴⁵

Access control is another rapidly expanding use for contact IC cards. They can be used for access to buildings, secure areas within buildings, computer systems, parking lots, or any other area. The logic ability and memory space combination allows the use of biometric identification. This provides sophisticated identification measures and significant security capabilities with unattended systems (limited human intervention) and without the use of a secure central database.

(b) Capabilities. The major advantage of programmable IC cards is their flexibility to adapt to a number of different applications. Even the diverse set of

⁴⁴ Biometric identification will be discussed further in Chapter IV.

⁴⁵ Department of Treasury, Financial Management Service, "Electric Benefit Transfer: Progress, Plans, Perspectives and People, EBT Status Report, August 1992, and Direct Payment Card: Midpoint Evaluation, March 31, 1993.

applications above can all be programmed into a single card. Programmable IC cards can be designed with secure operating systems and data integrity measures to make tampering, duplication, and modification extremely difficult. These cards are capable of full blown encryption algorithms, (such as RSA or DES described in the authentication section) at speeds greater than human response time.⁴⁶ This allows the positive identification and validation of the card/user to take place unattended and without the use of a central database.⁴⁷ With the exception of the OSs, the standards for contact IC programmable cards are well established.

(c) Limitations. Contact IC programmable cards are more expensive than other types of cards discussed thus far. Most IC programmable card applications utilize cards with 1-2 kilo-bytes (KB) of EPROM or EEPROM memory.⁴⁸ These cards cost about \$10.00 each. Currently, IC programmable cards are available with a maximum of 8 KB of memory and cost around \$20.00 per card. The CADs for these cards cost between \$200 and \$800 each depending on the capability required.⁴⁹

⁴⁶ Ondrusch, 1994, pp. 61-68.

⁴⁷ Nelson, R. A., "Authentication Techniques For Smart Cards," CardTech/SecurTech '94 Conference Proceedings, 1994, p. 47.

⁴⁸ A complete discussion of memory types is included in Appendix B.

⁴⁹ Seidman, Stephan, "The State of Smart Card Technology," CardTech/SecurTech '94 Conference Proceedings, 1994, p. 208.

While initial indications are that ICCs are more durable than magnetic stripe cards, they still have a limited life. The life expectancy is a function of the number of read/write cycles the card is subject to, because the physical contact of the cards terminals with the CAD eventually wears out these terminals. Like most other card technologies, programmable IC cards are subject to damage from chemicals, bending, flexing, scratches, heat, and demagnetization. The exposed contact points are also a source of potential damage.

(3) Memory IC Cards. Another major category of contact IC cards is memory IC cards. Contact memory-only IC cards have the same outward appearance as contact programmable IC cards, but have no or very limited logic capabilities. They instead use the entire chip area for memory space. Their physical operation and interface with the CAD is the same as a programmable card, with the exception of the operating system. On a memory-only card, the CAD performs the functions carried out by the OS in a programmable card. These CADs are sometimes referred to as *smart readers*.⁵⁰

(a) Common Applications. A major application of memory IC cards is the storing of data that does not require sophisticated security schemes. An example of this would be the storing of employee time and attendance records or medical information. These cards can be used in a distributed data environment, allowing all the required data to be stores on the card itself vice in a central database as we have seen with other technologies.

⁵⁰Seidman, Stephan, "Advanced Card Technologies," CardTech/SecurTech '93 Conference Proceedings, 1993, p. 21.

(b) Capabilities. Since memory IC cards use the entire chip for memory, they have several times the memory capacity of programmable IC cards. These cards are currently limited to 64 KB of memory, which is about 16 pages of text or eight times the amount of memory available on programmable ICCs. This vastly expanded memory capability gives these cards an entirely different set of capabilities. Memory-only IC card abilities are similar to the newer optical memory cards, however, optical memory cards have a larger data storage capacity.

(c) Limitations. The cost of memory IC cards, while less than programmable IC cards, is still greater than the other technologies discussed thus far. Durability limitations of IC memory-only cards is the same as IC programmable cards. While distributed data has its advantages, the distribution of data on cards is not flawless, since cards, and the data contained on them, can be easily lost or damaged. There must be elaborate backup schemes used with memory-only cards or the data lost will be difficult to regenerate. Memory-only cards provide less security than their programmable counter parts, and are inappropriate for use in applications requiring a high level of security.

(4) Super Smart Cards. A relatively new addition to the chip card arena is what is being termed a super smart card. This card contains a standard contact-type logic capable IC, a key pad, and a small display. They operate similar to standard programmable IC cards, with the exception of allowing input and output to occur directly on the card without the use of the CAD. These cards have not found mass appeal yet and are the

least developed of all chip card products.⁵¹ Figure 10 provides the layout of a typical super smart card.

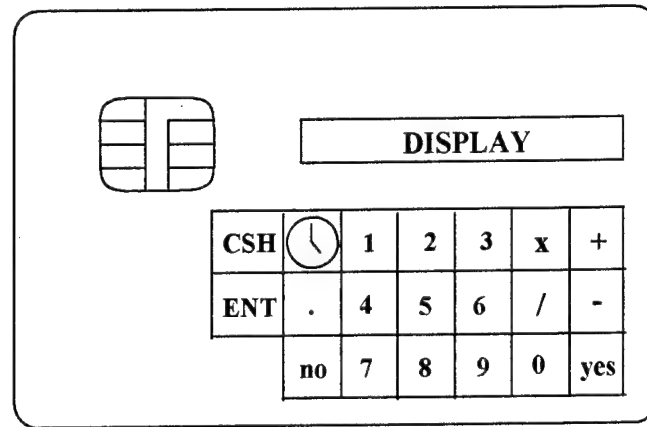


Figure 10 -- Super Smart Card

(a) Common Applications. Currently there are few common applications for this card technology. With the growing use of smart cards, this type of card may find favor in the niche of personal transactions between individuals, especially since CADs for this type of card would be relatively inexpensive.

(b) Capabilities. Super smart cards have the same abilities as standard programmable IC cards with the addition of allowing input and output (I/O) directly on the card. There seems to be little advantage to this technology, although some argue that it provides the card user with the assurance that their PIN is not being captured by the terminal and falsified values are not being written to the card without the users knowledge.⁵²

⁵¹ Seidman, "The State of Smart Card Technology," 1994, pp. 205-213.

⁵² Stanford, "What is a Smart Card," 1993, pp. 120-121.

(c) Limitations. These cards are prohibitively expensive, costing in excess of \$20 each. The same durability issues associated with other contact IC cards are present with super smart cards and, in addition, the durability of the display and key pad have yet to be proven. The super smart card provides another level of sophistication and the reliability of this card is lower than other IC cards.

d. Contactless Chip Cards

(1) System Description. Contactless chip cards communicate with a reader/writer, commonly referred to as a Card Coupling Device (CCD), through the use of an electromagnetic (EM) wave. Unlike contact cards they do not require contact terminals. Contactless cards, since they must possess the ability to transmit to the CCD, must have a power source. There are two options for this power source, building it into the card or delivering it to the card from an external source. Batteries are used for built in power supplies, and batteries thin enough to fit in the ISO standard 0.82 mm card are available. Battery life varies with usage, temperature, and other factors, and is limited. These batteries must be replaced every few years.⁵³ These cards are also commonly referred to as *active* contactless cards. The delivering of power to the card from an external source is known as inductive powering. Power is delivered in the form of an EM wave. There are several limitations involved with this choice of powering. First, the power cannot be transmitted over great distances efficiently. Second, the orientation of the

⁵³ Stanford, C.J., "Contactless Cards: An Overview," CardTech/SecurTech '93 Conference Proceedings, 1993, p. 86.

card to the CCD is more restrictive, usually ± 45 degrees. Third, radio frequency (RF) regulations may prevent the cards use in some areas.⁵⁴ These cards are referred to as *passive* contactless cards.

The distances that contactless card systems operate at vary from fractions of an inch to several feet. The shortest distance systems require the user to insert the card into a CCD, although the card does not make point to point contact with the CCD. These applications are referred to as a slot operation system. Another term the reader may encounter in the description of contactless systems is proximity cards or proximity badges. Proximity cards are contactless cards that operate at greater distances than slot operation cards, typically in the several inch range. Figure 11 provides a typical layout of a the card. The reader is reminded that these components normally lie between the plastic layers of the card, and may not be visible on the exterior of the card.

(2) IC Programmable Cards. Contactless IC programmable cards operate in much the same way that contact IC programmable cards work, with the exception of the physical contact points. The ICs in these cards have the same abilities as the ICs in contact cards. However, the applications, capabilities, and limitations of these cards are significantly different.

(a) Common Applications. Contactless programmable IC cards are extensively used in access control systems. Since these cards have the same functionality as contact programmable IC cards, the access control discussion also applies to these cards.

⁵⁴ Ibid.

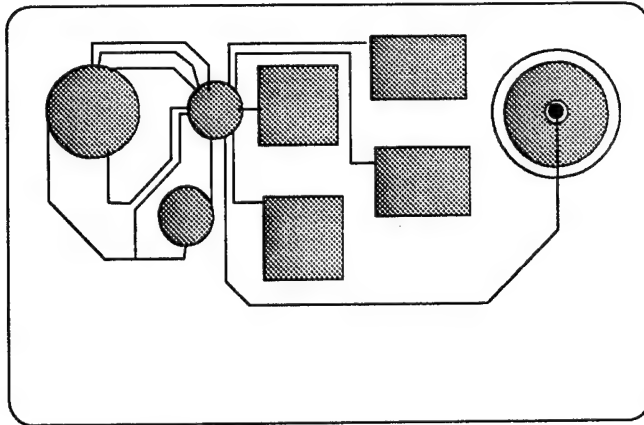


Figure 11 -- Contactless IC Card, Interior View

There is a significant amount of work being performed with these cards for the automated collection of tolls and traffic management. The collection of tolls uses a prepaid system which is then decremented as the driver passes through toll booths. The contactless card allows the driver to pass through the toll booth without stopping.

(b) Capabilities. A significant advantage of contactless cards is there is no contact between the CCD and the card, and therefore no contact points to wear out. Since no contact points are required, the entire IC and associated wiring can be well protected within the layers of plastic laminate. These two factors make contactless cards generally more durable than contact cards.⁵⁵

Since there is no need for direct contact with these cards, their use and application is more flexible, as seen with the toll booth example above. The battery operated cards provide more flexibility than cards which are powered by the CCD, because they do not require a certain orientation between the CCD and the card.

⁵⁵ Honold, Fred, "The Advantages of Contactless Cards," Smart Card Technology International, 1994, pp. 36-37.

(c) Limitations. The higher cost discussion of contact programmable IC cards is applicable here as well, with these cards costing slightly more than their contact brethren. While more durable than contact IC cards, contactless cards are still susceptible to damage from heat, flexing, demagnetization, chemicals, and the like. Contactless cards have a limited range, and this range is adversely affected by electro-magnetic interference (EMI). These cards cannot be used in areas where line of sight with the CCD is not possible or in areas with high EMI.

For battery operated cards, the limiting factor is battery life. With current technology, battery life on these cards is limited to a few years of intermittent use. The battery is normally not rechargeable nor replaceable, therefore these cards must be replaced at certain intervals.⁵⁶

(3) IC Memory Cards. These cards can be thought of as an advanced form of bar codes, to be used where the optical scanning of an identification tag is impossible or inappropriate.⁵⁷ These cards provide a fairly large storage area, up to about 64 KB, and with the exception of the requirement for physical contact with the CCD, are very similar in operation to the contact memory-only cards. Contactless IC memory cards are one form of proximity cards. Although other proprietary technologies have been used in proximity cards in the past, the contactless IC memory card is the most common form today. These cards are also similar in operation to the RF/ID tags discussed in the opening

⁵⁶ Pemberton, James, "Contactless Cards -- The Solution to All the Problems?", Smart Card Technology International, 1994, p. 85.

⁵⁷ Stanford, "Contactless Cards: An Overview," 1993, p. 84.

paragraphs of the chapter. These cards can be attached to containers, vehicles, inventory, or other items to provide automated tracking.

(a) Common Applications. Contactless memory-only IC cards major application is in tracking objects. These cards can respond with set codes when interrogated by a CCD. They can also store data when accessed by a CCD. The most common applications are in vehicle identification tags and toll collection. In contrast to programmable cards used for toll collection, memory-only cards only provide the CCD with an identification, the CCD then accesses the user's record in a central database and adds the appropriate toll charges to it. Billing is then done from this central database. Other applications are currently being investigated as well, such as scale bypass cards for trucks which have already been weighed.⁵⁸

(b) Capabilities. These cards have the same capabilities as the contact memory-only cards. They also have the advantage of not requiring direct contact as discussed under contact programmable IC card capabilities.

(c) Limitations. As discussed under contact memory-only cards, these cards have no logic capability for security. The discussion of battery life, distance, and EMI limitations under the programmable contactless IC card is applicable here as well.

⁵⁸ Department of Transportation, Nontechnical Constraints and Barriers to Implementation of Intelligent Vehicle-Highway Systems, A Report to Congress, June 24, 1994.

e. PCMCIA

(1) System Description. Personal Computer Memory Card Interface Adapter (PCMCIA) cards can be classified as a type of ICC, however, they only loosely resemble ICC cards. They are considerably thicker (from 3.3 mm to 10.5 mm vice 0.82 mm) and are have a hard plastic shell protecting the internal components. Because of this plastic shell, these cards do not under go the flexing and stresses that thin cards do, so they are not limited to single ICs per card, nor are they limited to 25 mm² square ICs. With multiple, larger ICs, it is possible to incorporate more functionality and memory into a single card. In addition, these cards uses two parallel 34-pin sets to form a sophisticated 68-pin interface (versus the simple contact points of other contact chip cards) to communicate with the CAD. The combination of these abilities gives the PCMCIA card far more capability than standard thin cards. These cards are currently available in up to 80 MB memory configurations, providing a type of hard drive ability for palmtop computers, printers, notebook computers, personal digital assistants and other small devices. PCMCIA cards are also available to carry out interface functions such as fax/modems and network communications. These cards can also be loaded with software applications for execution on these small devices.

There are currently three standard sizes for PCMCIA cards. All are the ISO standard height of 85.6 mm and width of 53.98 mm, but vary in thickness. Type I is 3.3 mm thick, Type II is 5 mm thick and Type III is 10.5 mm thick. Because the 68-pin interface is common to all types, each type is backward compatible with the previous

type(s). This means a Type II can accept a Type I card, and a Type III can accept Type I or Type II cards.

(2) Common Applications. The most common applications for PCMCIA cards are in the small computing environment where a 3 1/2 inch drive is impractical. As the use of these products rapidly expands, so is the number and types of PCMCIA cards being offered. They have yet to penetrate the common thin applications, due mostly to their high cost and capability beyond what thin card systems developers currently know how to apply. As their price decreases, the infrastructure of CADs grows, and the need for more ability increases, these cards are certainly poised to provide the capabilities required.

(3) Capabilities. With well protected, multiple, large ICs, and a able interface, these cards can provide significant capabilities. With the current state of micro-circuitry, almost any application is possible within these cards. Standards are well defined for these cards and compatibility between devices is not a significant problem.

(4) Limitations. The most significant limitation of PCMCIA cards is their high cost. The relatively small, 2 MB PCMCIA cards are around \$100 each, and more capable 64 MB cards are over \$500.⁵⁹ Specific application cards such as fax modems are also in the hundreds of dollars.

Like other contact cards, PCMCIA cards make physical contact with the CAD, and although the 68 pin connector is very durable, it can wear out or be damaged.

⁵⁹ Haddock, 1993, p. 389.

A contactless PCMCIA card has yet to be produced. The thickness of PCMCIA cards make the carrying of them not as practical as thin card technologies that fit conveniently with existing credit cards and ATM cards of the same size.

A concern in the security arena is that intra-IC communications must be encrypted or be subject to possible interception and duplication. With the larger ICs, it would be possible to conduct encrypted intra-IC communications, however, there would be some degradation in speed.

5. OPTICAL MEMORY CARDS

a. History

The use of optical media as a storage device began in the late 1970s. The first large scale uses of this technology were in videodiscs and compact discs (CDs). The videodiscs were not well received by the public for two reasons; consumers insisted on being able to record their own material, and there were good substitutes available at lower cost (video tapes). However, the infrastructure of CD players quickly spread during the 1980s, due to the higher quality and relatively low cost of these machines.⁶⁰ This wide spread commercial use of optical media lead to advanced research in this area. The first widespread use of optical media to record data occurred in the late 1970s. Optical memory cards (OMCs), were introduced in 1981. These cards are also commonly referred to as Laser Optical Memory Cards (LOMCs).

⁶⁰Bitter, Gary G., (ed.), Macmillan Encyclopedia of Computers, Macmillan, NY, Vol. 2, 1992, pp. 955-960.

b. System Description

OMCs use the standard plastic card, and cover the surface with a thin layer of optical media similar to the surface of a CD. The optical layer is covered by a transparent layer of polycarbonate, providing protection for the optical layer. The storage of data on these cards occurs by placing microscopic pits, or "spots", on parallel tracks of the optical layer. The presence or absence of these spots indicate the binary "1s" or "0s", and can then be read as data by a laser beam.⁶¹ OMCs use what is known as write once, read many (WORM) technology. This means once the optical media has been written to, it cannot be changed. Figure 12 provides a typical layout of an OMC.

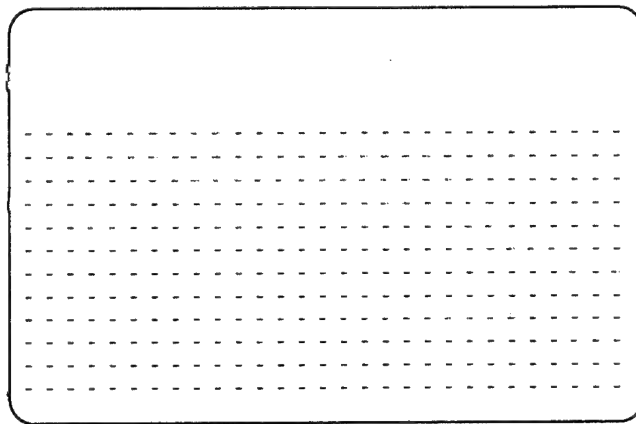


Figure 12 - Optical Memory Card

c. Common Applications

The most common application for OMCs is in the storing of medical information. The high data capacity lends itself well to this application, for medical records tend to be lengthy, especially when they include items like x-ray images, cat scans, ultrasounds,

⁶¹ Stanford, "What is a Smart Card," 1993, p. 120.

or other imaging technologies. These cards can be used anywhere there is a need for portability of large document storage. They are being applied to library systems, inventory management and control, and even pay telephone systems.

d. Capabilities

OMCs have the highest data capacity of any card technology currently on the market, with 2-16 MB of storage. The amount of storage available on the card is a function of the size of the data spots. Current laser and optical media technology uses spots as small as 2.25 micros, allowing 16 MB of storage. OMCs are also the most durable of the current card technologies. They are unaffected by magnetization, heat and cold (-40 to 212 degrees), EMI, flexing, and weather. They are still damaged by scratching, but data which is not directly where the scratch is can be recovered, making them the most resilient of the card technologies.

Although the cards are not updatable, with the vast storage ability of OMCs, new data can be written to a different area on the card. This is known as directly read after writing (DRAW). When new data is entered on the card, a pointer to this data is updated to reflect the location of the most up-to-date information, but the old information cannot be erased. This provides a audit trail of all previous information, which can easily be reconstructed. The use of DRAW-type cards provides the user and the application with the appearance of updatability.

e. Limitations

OMC costs are comparable with the ICC costs, at around \$4.00 each with 2-4 MB of storage. The readers/writers are considerably more expensive, currently costing several thousand dollars, however read only units are available for hundreds of dollars.⁶²

Security is an issue with these cards. The audit trail provides an excellent source of validating the authenticity of the card, and the vast storage area allows the storing of biometric identification data. The duplication of these cards is relatively simple, however, the updating of data, especially encrypted data is not easy.

The standards for OMCs have only recently been completed. As OMC technology is still in its infancy, the infrastructure and vendor support is not yet well established. As this capable technology matures, these will also.

6. HYBRID TECHNOLOGY

a. History

For most of the above technologies, there are standards which state the exact locations of the media, embossing, contact points, etc. The only exception is bar codes, which are normally read by a hand scanner or a fixed scanner which the cards are passed over, thus eliminating the need for the bar code to be at an exact location on the card. Most of these standards, by not indicating the same placement for the technologies, allow

⁶² Capaldi, Lucy, "The Defense Logistics Agency Automated Manifest System: A Status Report," CardTech/SecurTech '94 Conference Proceedings, 1994, p. 299, and Stanford, "What is a Smart Card," 1993, p. 121.

multiple technologies placed on a single card to still conform to standards. Currently, the most common hybrid cards are bar codes and/or magnetic stripes placed with an IC.

b. System Description

It would be fruitless to attempt to describe all the systems which are possible using hybrid technology. The operation of these cards, with the exception of possible interfaces between the various technologies, would be similar to the individual systems alone. The possible interfaces between different technologies is yet to be seen. A card that is possible using hybrid technology is provided in Figure 13.

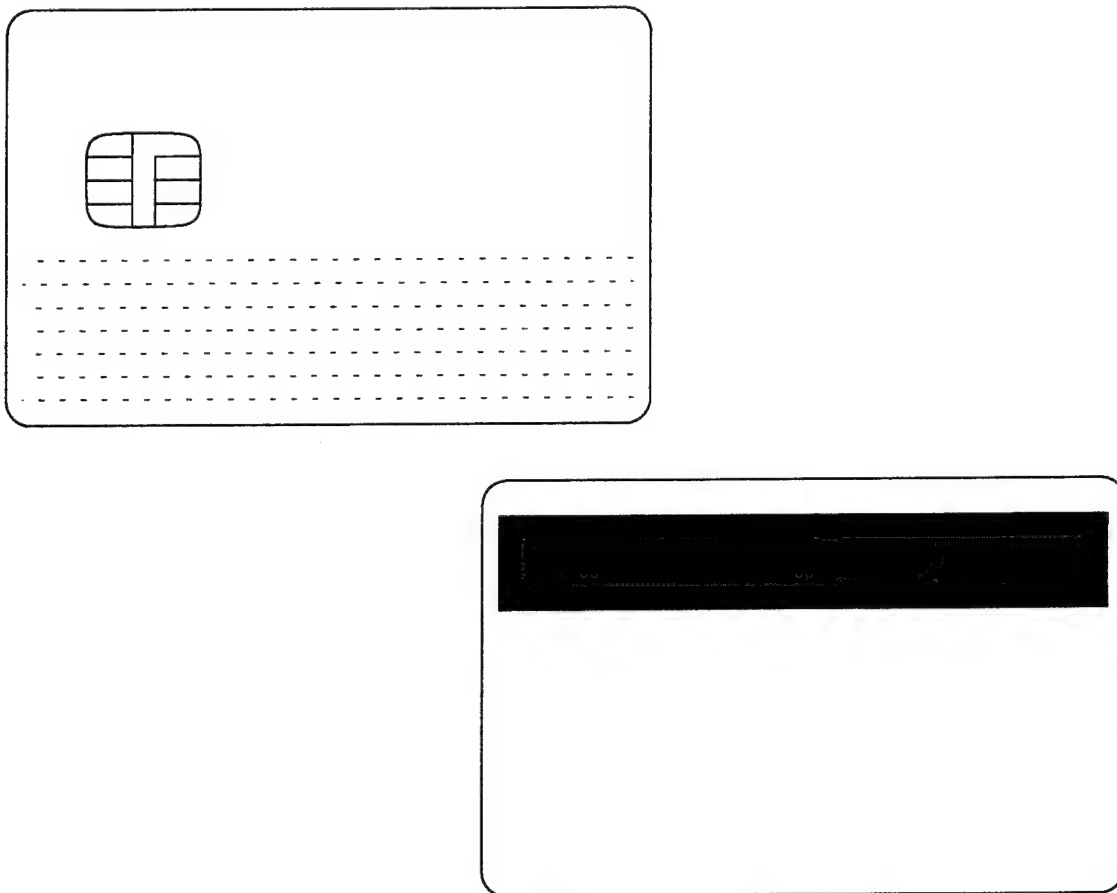


Figure 13 -- Hybrid Technology Card - Front And Back

c. Common Applications

Hybrid technology is still in its infancy. With the endless possible combinations of technology comes an endless array of possible uses, constrained only by the imagination of the systems developer. The lack of a standard specifically for hybrid technology may hinder some of the more creative applications, especially where the various technologies need to interact to produce the most efficient use of the limited card space.

d. Capabilities

The capabilities of the various combinations would be at least the sum of the capabilities of the individual technologies. Combinations where the technologies interface, such as a combination of a programmable IC with an optical storage space, could provide a greater advantage than the technologies alone.

With a hybrid card, it is possible to have an independent backup systems to exist on the same card, thus reducing the chance of failure. Hybrid cards also allow multiple applications to exist on a single card and allow them to use the most appropriate media choice for that application.

e. Limitations

The lack of standards for multiple technologies is a severe limitation. Currently each individual technology has its set of standards, but there are not standards addressing the interoperability of multiple technologies on a single card. This forces each technology to act independently, or the CAD to act as the coordinating mechanism. The international standards bodies will surely address this in future standards.

Cost is another limitation of this technology. Cards will always be subject to loss, damage, theft, etc., and the cost of cards with multiple sophisticated technologies on them will be significant. There can be significant amount of data stored on these cards as well, and if not constantly backed up, recreation of lost data could be costly.

D. SUMMARY

This chapter presented a discussion of current card technologies. Table 1 provides a summary of the key elements of these technologies. The recent increased rate of technological change, ever increasing array of card technologies available to choose from, and evolutionary nature of these card technologies makes choosing the most appropriate system difficult. The framework presented in Chapter VI will aid the decision maker in procuring the most cost effective solution for the application.

TABLE 1 - SUMMARY OF CARD TECHNOLOGIES⁶³

Technology	Memory Capacity	Card Security	Card Costs	CAD Costs	Logic Capability
Bar Codes	32 bytes (40 char)	low	\$0.03 - 0.08	\$100	no
Magnetic Stripe	320 bytes (475 char)	low	\$0.08 - 0.30	\$25 - 500*	no
Wiegand	56 bits	medium	\$0.50 - 2	\$20	no
ICC: Contact Programmable	8 KB	high	\$2.50 - 5	\$200 - 800*	yes
Contact Memory	64 KB	limited	\$0.50 - 2	\$20 - 400*	no
Contactless Programmable	8 KB	high	\$3.50 - 6	\$300 - 1000*	yes
Contactless Memory	64 KB	limited	\$1 - 2	\$30 - 500*	no
Super Smart	8 KB	high	\$20+	\$150 - 900*	yes
PCMCIA	80 MB	very high	\$100+	\$30- \$1000#	yes
Optical Memory	16 MB	limited	\$2 - 10	\$400- 3000*	no
Hybrid - depends on combination used	up to 16 MB	can be high	\$2 - 20	\$1000s	can be

* depending if read only or read/write

depending if embedded or stand alone

⁶³ Compiled from a variety of sources.

IV. AUTHENTICATION TECHNIQUES

A. INTRODUCTION

Although card technologies can be used as stand alone systems, they provide little security in this configuration. For a card system to provide security, there must be some manner of ensuring the person who is currently possessing the card is the person who is authorized to use the card. The system must also validate that the card being presented has not been altered. To accomplish this, card systems are frequently used in conjunction with some form of identification or authentication of the person using the card and of the card itself. This chapter discusses the common authentication techniques for cards and for individuals, by mechanical and human means.

A major benefit card systems can provide is automation capability, the ability to reduce the human intervention required. Therefore, the discussion of authentication accomplished by human intervention is brief and provided only for completeness. Automated authentication techniques such as biometric, behavioral, and others provide a more capable system and are discussed in depth. The identification of the cards is accomplished by a variety of proprietary means, the more capable the card is, the more sophisticated the identification scheme can be.

B. BACKGROUND

The authentication process is generally considered to consist of one or more of the three types of identification methods. The three types of identification methods are:

1. What the user possesses
2. What the user knows
3. Who the user is¹

What the user possesses, refers to some form of token, be it a license, a badge, a card, a ticket, or any other form of token. While this token can take many shapes, this paper only discusses tokens in the form of card technologies. Tokens can be forged, so they must be authenticated. Token authentication for the more advanced card technologies, (cards with logic capability or large data storage areas) can be very sophisticated. A discussion of these authentication schemes is beyond the scope of this paper and will not be presented. However, a brief overview of some card authentication schemes for less capable cards has been included. These include technologies such as electronically verifiable holograms, magnetic ink, and optical character recognition. Authentication systems which use only this first identification method are relatively insecure, allowing access to anyone who possesses the right token.

What the user knows, refers to some form of password. Again, these can take many shapes, from static character strings and personal identification numbers (PINs) to challenge and response systems. The more dynamic the password is, the more security it

¹ Muir, Barbara, "Authentication Considerations For External User Access," CardTech/SecurTech '93 Conference Proceedings, 1993, p. 900.

provides. Systems using only what the user knows likewise provide limited security, allowing access to anyone possessing the right knowledge.

Who the user is, refers to some form of positively identifying the individual. These systems can take one of two forms, behavioral and physiological. Behavioral characteristics are features that result from how an individual performs some function, such as signing their name or typing a string of characters. Physiological features are biological features about the person that distinguished them from others. These include features such as fingerprints, hand geometry, eye retinal pattern, hand vein patterns, or facial geometry.² Voice recognition systems fall into both categories, since it includes both behavioral aspects (accent) and physiological features (vocal cord shape).³ For the purpose of this paper, and in compliance with industry norms,⁴ voice recognition systems will be considered a behavioral attribute.

Figure 14 provides a graphical view of the three different authentication methods and some of their enabling technologies. While understanding of these three authentication methods by themselves is essential, their true capability is achieved when used in

²Holmes, James, P., "Promising Developments and Biometric Testing," CardTech/SecurTech '93 Conference Proceedings, 1993, p. 317 and Carter, Bob, "The Present and Future State of Biometric Technology, CardTech/SecurTech '94 Conference Proceedings, 1994, pp. 402-405.

³Alexandre, Thomas and Vincent Cordonnier, "An Object-Oriented Approach for Implementing Biometrics in Smartcards," CardTech/SecurTech '94 Conference Proceedings, 1994, p. 150.

⁴Revillet, Marie and Mohammed Achemlal, "Biometric Authentication Principals, Use and Limitations," CardTech/SecurTech '94 Conference Proceedings, 1994, p. 161.

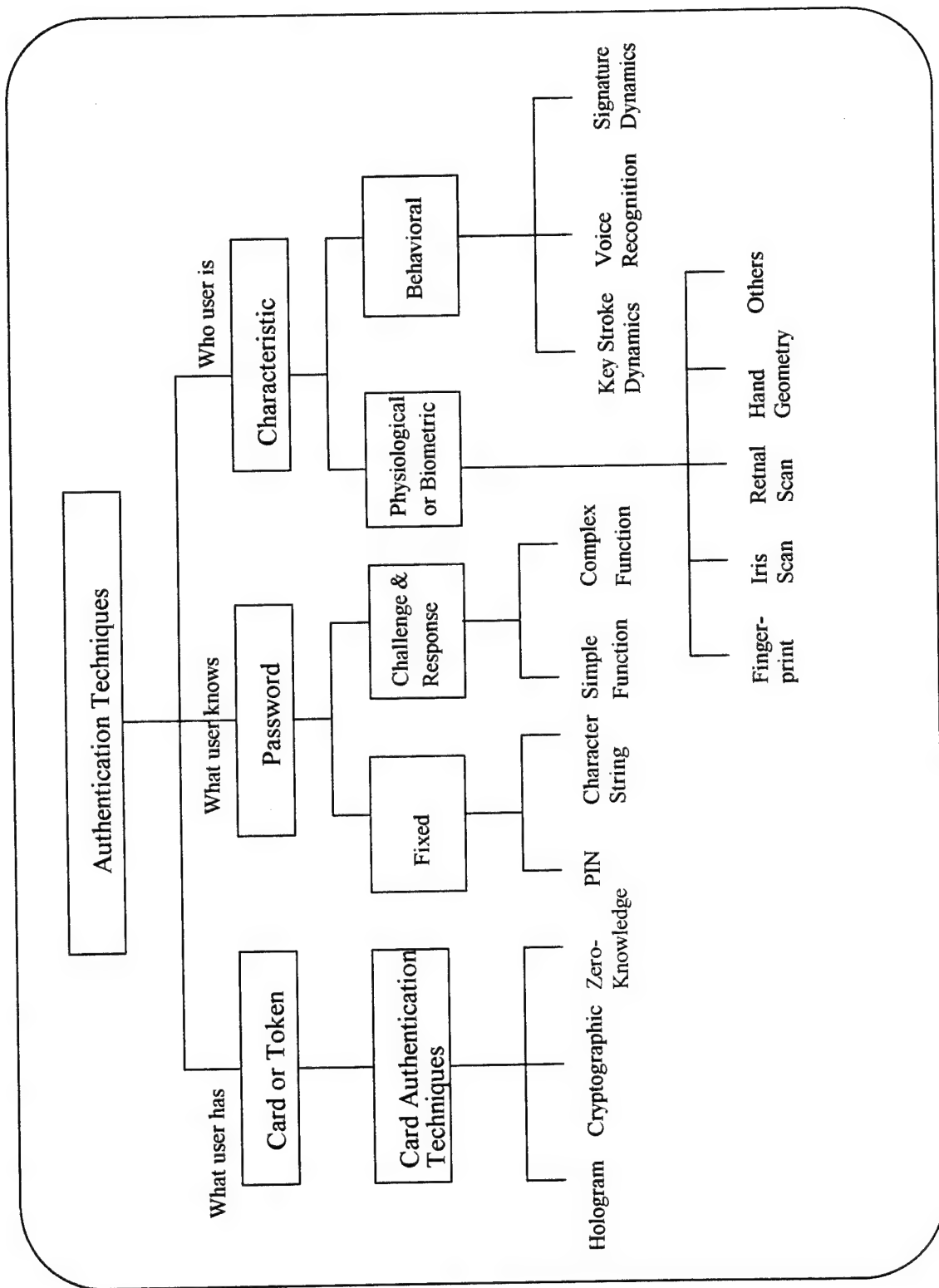


Figure 14 -- Authentication Hierarchy

combination. There are seven possible combinations which use one or more technology, they are: The three methods alone; the three combinations using two methods; and the use of all three methods together. The most common systems are a combination of two technologies, and include such familiar applications as ATM machines (which use a card and a PIN), and access devices (using a card and a biometric authentication). Adding a second authentication method does not necessarily increase the security of the system, as in the case of a card and static PIN, an impostor can be in possession of both. Combining biometric authentication with a token makes the identification of the individual easier (in terms of speed, processing requirements, data storage, etc.) by changing the problem from one of identification to one of authentication.

A discussion of identification and authentication is useful here. Identification and authentication are actually two different concepts, although the terms are often used interchangeably. In an identification system (also sometimes called recognition systems), the attribute is entered without any information about the individual. The system attempts to match the attribute in its large database of stored attribute-identity combinations. These systems are commonly used by law enforcement officials to identify criminals. These systems are large, costly, and have a higher computational ability than authentication systems. An authentication (also referred to as verification) of a person is the verification of the identity they claim to have. These systems use some form of identification (such as a card, access name, or other identity claim), and an identifier (such as a password, personal

identification number, or physical characteristic). If the identifier matches the reference stored in the system's database, authentication is positive and access is granted.⁵

To complete an authentication, there must be a means of comparing the person currently being presented to the "actual" or reference data about the person issued the card. Actual or reference data is normally captured at time of enrollment in the system. This comparison can be accomplished in one of two ways. In a distributed system, the reference data is stored directly on the card. This data must be protected in some way, such as by using one of the data encryption techniques discussed in Chapter II. The data must either be protected from replacement, by using unalterable data areas for example, or the system must be able to detect replacement, such as by audit trail use. In a non-distributed environment the reference data is stored in a central data base. When an authentication request is received, the system compares the current data to stored data and determines if the authentication of the person is valid. A similar system can be used to implement multiple access levels into a single system. After the authentication of the individual, the system could then authenticate the individual's access to an area, system, or procedure. The access authentication can be distributed or not, just as the reference data is. A hybrid data storage scheme, where the authentication information is contained on the card and access information is stored in a central database, is also possible. This is a common configuration when a single card is to be used to access multiple systems.

⁵Revillet, 1994, pp. 159-160.

C. AUTHENTICATION BY HUMAN INTERVENTION (MANUAL)

1. Authentication of the Individual

People often use visual cues for authentication techniques. This use of visual authentication has been in use since the beginning of time. Cave men were able to distinguish fellow humans from animals and would act accordingly. Humans are very good at recognizing individuals they know and their ability for pattern recognition is unmatched by any automated process. However, humans are not as good at tasks that require long hours of attention to a mundane chore.⁶ To have a human controlled system that is available 24 hours a day, 365 days a year requires a great deal of human capital. The cost of human capital, demand for constant system availability, and poor performance of humans at mundane chores are major factors that have driven the use of automated authentication. The most common forms of identification by human intervention are discussed below.

a. Photograph

Attaching a photograph to a card technology and verifying the person's visual appearance each time they use the card provides a low level of security. There are many negative aspects to this type of authentication. People change their appearance over time, including changing hair length and style, facial hair, glasses, etc. Depending on the reissue frequency of the card, they may not closely resemble their picture at all. This degrades the ability of the person checking the card to properly perform their function. In addition, some humans have an exact twin, and it may be difficult to distinguish them based on

⁶Holmes, 1993, p. 318.

outward appearance alone. Pictures are also relatively easy to alter or remove and replace. There are many new technologies being developed which strive to minimize this, including holographic images, or seals added directly into the laminating material of the card. While these provide some security against altering, they are again limited by the abilities of the person who checks them.

b. Signature Block

A signature block is frequently added to the back of a credit card. This signature block is signed by the authorized user when they receive the card. There are a number of problems associated with this form of authentication. If the card is intercepted before being signed, either in delivery of the card, or if the user forgets to sign it, an unauthorized user can sign it and use the card. Another problem is that ink is easily removed from the signature block and again the unauthorized user can sign it and use it. A final problem is that signatures can easily be copied. Since the unauthorized user can see what the signature is supposed to look like, he can spend a few moments perfecting the signature and duplicate it. Expecting a person to differentiate between the signature on the card and the one being presented may be beyond the human capability. Some newer cards allow the electronic recording of the signature on the card, under the laminate. While this helps by making the signature more difficult to alter, it does not eliminate the possibility of copying the signature.

2. Authentication of the Access Device

As with the authentication of the individual, the human authentication of the access device uses visual cues. The visual appearance of the card must be easily recognizable to the authenticator. Several technologies aid in this visual identification.

a. Name Embossing

Name embossing on cards has been used since the charge-a-plates of the 1950s. This technology provides some authentication ability of the access device, but its use is limited. The undetectable changing of the name embossed on a card is relatively difficult and would provide minimal advantage. Name embossing is much more often used as a convenient form of data capture rather than a true authenticating method.

b. Holographic Seals and Images

The physical appearance of the card is the most common visual authentication cue. The plastic material of the card can contain dyes and designs which are difficult to duplicate. A recent addition is the use of holographic seals added to the card. These holograms, while relatively inexpensive to mass produce, are difficult and expensive to forge. Images can also be added to the layers of laminate, making the opening, altering, and resealing of the cards difficult. While these methods do provide some protection against counterfeiting, they still rely on the person checking the card to make the decision that it is genuine. It also still relies on the individual's ability to correctly authenticate the user.

Recent developments in holographic imaging include the advent of machine verifiable holograms. These holograms are discussed under the *machine authentication of the access device* section of this chapter.

D. AUTHENTICATION BY MACHINE (AUTOMATED)

1. Authentication of the Individual

a. Personal Identification Number or Password

(1) Fixed. The most common form of *what the user knows* authentication is the Personal Identification Number (PIN) or password. With this type of authentication, a card holder is issued or selects a fixed length of numeric or alphanumeric characters. Depending on the system these may be from four to ten or more characters in length. They may be numbers only, letters only, or any character including punctuation and symbols. The user enters this string when queried by the authentication device. This form of authentication is also very insecure. It allows anyone knowing the fixed character string to be authenticated. PINs or passwords can be easily obtained by observing the authorized user entering it at the key pad, by guessing, by brute attack, or by obtaining it from the system. PINs and passwords change relatively infrequently, adding to the low authentication abilities of this type of system.

(2) Challenge and Response Systems. Challenge and response systems are also known as one-time password systems, because the password changes every time the system is accessed. This system uses a static mathematical or logical function instead of the standard static character string. The system challenges the user with a number or

character set. The user performs the function on this challenge and responds with the correct password. The system authenticates the user based on their response. One-time passwords are more secure than static passwords or PINs, since the password is changing each time, making the interception of a password useless. However, their usefulness is limited by the complexity of algorithms people can remember.⁷ Some systems use more complicated functions which are programmed into hand-held devices. However, as easily as a token can be lost or stolen, so can these hand-held devices.

b. Physiological (Biometrics)

Biometric identification, in the form of fingerprint analysis, has been used for over 100 years. However, it was not until the early 1970s that an automated form of biometric identification emerged. These earliest automated systems were hand geometry systems. Automated fingerprinting systems did not emerge until the late 1970s.⁸

Unlike PIN or password systems, biometric systems do not have a clear *yes/no* answer each time a verification is attempted. With a PIN or password, the user either has it correct or not. In a biometric authentication system, the image to be authenticated will rarely produce an exact match with the reference image. This is not because the attributes change that frequently, but rather because the recording of the image will vary slightly each time. The attribute will be placed at a slightly different angle, with different pressure,

⁷Pfleeger, Charles, P., Security in Computing, Prentice Hall, Englewood Cliffs, NJ, 1989, pp. 233-234.

⁸Miller, Benjamin, "Biometric Identification: The Power to Protect People, Places and Privacy," CardTech/SecurTech '94 Conference Proceedings, 1994, pp. 193-201.

and there will be different contaminants on the recording device as well as the attribute. Therefore, these systems must operate in gray areas, and a confidence level must be used to determine whether the attribute matches or not. Physiological biometrics produce more consistent sampling than the behavioral techniques do.⁹

There are many methods of capturing biometric data and matching it with a previously captured image. These techniques include digitizing of imaged features, least squares fits, filtering, Fourier transforms, and neural methods of pattern recognition. Most of these techniques are well guarded secrets of the device manufacturers,¹⁰ so it will not be possible to provide a complete discussion of the intricacies of each system's operations. Instead, this section will discuss the basic operation of the system, and some of the relevant issues in using the system. Where available performance figures, in the form of false rejection rates (FRRs) and false acceptance rates (FARs), are provided. As discussed in Chapter II, a FRR is the rejection of a valid user, and FAR is the authentication of an unauthorized user.

A brief discussion of *neural networks* is appropriate at this point. Unlike conventional data processing techniques, neural networks are "trained" rather than programmed. They develop their own solutions to problems through exposure to examples. In this manner it is possible for a system to learn. An example is neural network use in training a device to recognize a person's handwriting and being able to convert it to typed

⁹Carter, 1994, p. 403.

¹⁰Holmes, 1993, p. 319.

text. The longer the person uses the system, the better the system's recognition of their handwriting becomes. Neural networks are well suited to biometric authentication because they can learn to adapt to biometric features that slowly change over time.¹¹

(1) Fingerprint. Fingerprinting is the most widely used biometric identification technique.¹² The fingerprint is an excellent attribute to base an identification system on since it is stable and unique from birth to death. The chance of two people having the same fingerprints is less than one in one billion.¹³ Fingerprint systems use a variety of different techniques to form templates using data from the print's end points, junctions, locations, relative geometry, and number of ridges.¹⁴ This process is referred to as *minutiae matching*. The data required to perform a minutiae match can be collected in a number of different ways, the most common being based on frustrated total internal reflection spectroscopy (FTIR). This uses a light source which shines on the finger being presented. The reflected light is then collected by a photo detector and evaluated. Recent use of ultrasound imaging for fingerprints as well as other biometrics has shown promising results.

Because of its long time use in law enforcement applications, there is a general stigmatism around fingerprints as a form of authentication. Fingerprints left at a

¹¹ Sheppard, Colin, "A Neural Network Approach to Fingerprint Verification," CardTech/SecurTech '94 Conference Proceedings, 1994, p. 185.

¹² Ibid., p. 183.

¹³ Miller, 1994, p. 197.

¹⁴ Ibid.

crime scene have been used to convict many criminals. In contrast to many other biometric identifiers, fingerprints can be left on almost any surface. Most other biometric identification methods require the use of a sophisticated reader, and cannot be collected without the individual present and in close contact with the reader. While this may be an advantage in some systems, such as deterring the receipt of multiple food stamp benefits, it is a disadvantage in systems where strong user acceptance is desired.¹⁵

Skin surface conditions adversely effect quality of a fingerprint scan. Common elements found on the finger can severely degrade recognition performance, such as dirt or oil in the ridge valleys, damage due to injury, or worn down ridges due to a person's occupation.¹⁶ People also purposely alter their fingerprint appearance through the use of chemicals. Fingerprint readers also cannot distinguish between a living finger, and a latex copy or one that has been removed from the body.

Current fingerprint systems have a false rejection rate of about three percent, and false acceptance rates of around one in one million. These capable fingerprint systems require between 750 and 1,000 data bytes to represent an accurate template.¹⁷ However, a technique has been developed which can match a fingerprint in as little as 918 data bits (just over 100 bytes), small enough to be saved in tracks 1 and 3 of an ISO standard magnetic stripe card.¹⁸ The reliability of these systems is yet to be determined.

¹⁵ Ibid., p. 198.

¹⁶ Schneider, J.K., "Ultrasound for Biometric Capture," CardTech/SecurTech '93 Conference Proceedings, 1993, p. 333.

¹⁷ Miller, 1994, p. 197.

(2) Hand Geometry Recognition. A hand geometry recognition system uses the lengths, widths and/or thickness of the hand and/or fingers to create a unique template for each individual. These systems may use anywhere from a dozen to several hundred points to construct this unique template. A hand geometry recognition reader normally provides a plate on which to place one's hand, and may even include pegs to aid with the proper placement of the hand for reading.¹⁹ A variety of methods for reading the hand geometry are currently being used, including laser, photo-imaging, and ultrasound. These systems are able to measure lengths within thousandths of an inch. The more sophisticated the system, and the greater the number of points it samples to construct its template, the greater the security, and the fewer the FAR and FRR errors. It is possible that two individuals can have hands of the same dimensions, but the more data that is collected about the hand the less chance there is for commonalties. This author's research indicates hand geometry appears to be less unique than other biometric characteristics.

The major drawback to hand geometry is the expected change over time. As the body ages, the hand will change shape. In addition, injury and swelling due to water retention, or weight gain can significantly influence the shape of the hand. There is a small portion of the population for whom this technique would not be appropriate, such as amputees and people with certain birth defects. Similar to fingerprint systems, hand

¹⁸Hollington, Jack, "Automated Fingerprint Analysis Offers Fast Verification," Sensor Review, Vol. 12, No. 3, March 1992, pp. 12-15.

¹⁹Recognition Systems, Inc., ID3D HandKey Brochure, 1994.

geometry systems cannot distinguish between a living hand and a latex copy or one which has been removed from the user.

This type of recognition is a non-invasive measurement and has a high user acceptance. Users are comfortable with the system because the scan is done with them maintaining full view of their hand. It is also not an identifying characteristic outside of the scanner. Users are less likely to feel their hand geometry will be used for other purposes. Hand geometry systems are unaffected by dirt, cuts, and other minor skin variations. Newer hand geometry readers use both the top and side views of the hand to form a template. Reference templates for hand geometry are under 10 bytes, the smallest of any biometric authentication technique.²⁰ However, there is some reluctance with this technology, stemming from a lack of confidence in the differentiation ability of hand geometry and the fact that this technology is old. While the more capable hand geometry system have accuracy and differentiation results rivaling any other biometric,²¹ they are often shunned for "more advanced technologies."

(3) Retinal Scan. The blood vessels on the rear of the eye, the retina, form a unique pattern. Retinal scans are performed by directing an infrared light source through the pupil to the retina. The reflected pattern is captured by a camera and converted into a unique template. Reference templates for retinal scans are about 35 bytes in size,²² which

²⁰ Miller, 1994, p. 198.

²¹ Recognition Systems, Inc., 1994.

²² Miller, 1994, p. 198.

is considerably less than most other biometric techniques. There is some fear of damage to the eye and vision associated with the long term use of these systems. While there has been no evidence to support this, the public fear still exists. The difficulty involved in duplicating these minute patterns on the rear of the eye results in a higher level of system security. Retinal scanners are also better at detecting non-living presentations, since most systems require the user to focus on a point in order to provide the correct representation.

(4) Iris Scan. Iris scan is similar in operation to a retinal scan, however it images the front of the eye or iris features. The patterns of flecks on the iris provide as unique a pattern as any other biometric technique.

Iris scans use a video image to capture the pattern. This video image does not require the user to focus on a target, nor does it require the use of infrared light, and it can be accomplished at distances as great as a few feet.²³ This has lead iris scan technology to meet with greater public approval. This distance factor has allowed the general public to feel more comfortable with the belief that there will not be any damage to the eye. This system also has an advantage in that it can differentiate between a living eye and a deceased or reproduced eye by the constant variations in pupil size of the human eye.

Currently, iris scan technology is just emerging, with the first products expected to reach market late in 1994.²⁴ The size of the data required for reference images

²³ Ibid.

²⁴ Ibid.

and the FRR/FAR data remains to be seen, however it is expected to be about the same size as a retinal scan.

(5) Face Recognition. There are several facial feature recognition systems under development. These systems use a form of machine vision to develop pattern recognition. Machine vision, in combination with infrared scans of facial temperatures is also being investigated. There are several complicating aspects of facial recognition, including facial expression, beards, haircuts, makeup and the like. There is a great deal of interest and work being conducted in this field, however currently there are few products on the market.²⁵ Time will tell if face recognition is a viable, secure biometric authentication technique or not.

(6) Hand Vein Patterns. Hand vein pattern recognition technology is a relatively new technology which likewise has few marketable products. Most work in this area is focusing on the use of ultrasound to obtain the unique pattern of the veins in the wrist and/or hand. The user acceptance, error rates, cost, and uniqueness of the patterns obtained in this relatively new technology remain to be seen.

(7) Other Technologies. Most other biometric identification technologies are still too large and cumbersome to be used in an authentication environment. These include things like DNA sampling, hair analysis, blood matching, skin samples, dental records, and the like. The majority of these methods are currently reserved for crime scene analysis and criminal prosecutions, where time and financial constraints are not an issue. However, in

²⁵ Ibid., pp. 200-201.

the future these techniques may evolve far enough to become viable card authentication techniques.

The use of ultrasound for biometric imaging appears to be possible in the near future. It can be used for fingerprint,²⁶ and hand vein pattern recognition. Currently, ultrasonic imaging is prohibitively expensive. Recently, ultrasound technology has made great advances in capability and decreases in price. As the medical uses for ultrasound increase the demand and volume of ultrasound devices, the cost should decrease. Ultrasonic imaging may be a cost effective authentication alternative in the near future.

c. Behavioral

(1) Signature Dynamics Verification. Signature dynamic verification systems, like many other authentication systems, can be designed in a number of ways to capture any number of different aspects of the signature. To construct a template for the signature, the most common form uses three data fields; the two-dimensional representation of the signature, and time. From the two dimensional signature and time values, the speed that the person is signing can be calculated.²⁷ Some more capable systems may also use amount of pressure with the paper, but this is relatively difficult and expensive to capture, measure, and analyze with current technology.

These systems are relatively secure in that they capture sufficient amount of data to make the signature truly unique. They also eliminate some of the problems

²⁶ Schneider, 1993, p. 333.

²⁷ Alexandre, 1994, p. 151.

associated with human signature verification by using the time component. While it may be easy to learn to forge someone's signature, it is much more difficult to be able to do so with the same speed and pen strokes.

Signatures change and evolve over time. Current technology, in the form of neural networks, allow the signature verification device to "learn" these evolutions. They can allow slight changes in the signature with successive accesses and can continually update the base signature. These systems are subject to the normal injury and physical disability related problems that plague other systems.

(2) Keystroke Dynamics. Keystroke dynamics (also called typing rhythms) analyze the typing styles of different individuals. These analysis can be constantly taking place in the background on a system. The requirement for users to type long strings of characters causes this system to be of limited use in access control situations where authentication must take place in seconds. However, this technology is eagerly awaited by computer security professionals,²⁸ where longer typing times are common and access needs to be constantly monitored.

(3) Voice Recognition. Voice recognition is accomplished by converting sounds spoken by humans into electrical signals. Current voice recognition systems use information derived from acoustic measurements of speech. These include parameters of pitch, spectral magnitudes, formant frequencies (resonant frequencies of the vocal track), and energy profiles.²⁹ These parameters are then compared to the recorded voice pattern

²⁸ Miller, 1994, p. 200.

of the authorized user. Different systems employ one or more of these measurements to carry out the verification or authentication. These systems pattern match the speech signal, as a time-ordered set of features, to a stored template. Templates can be composed of multiple words, a single word, syllables, or phonemes. Most systems use either single or multiple words. The input utterance template is then compared with the reference template by aligning the two templates at equivalent points in time. Some stretching or compression of the time in the template may be necessary, or the time dimension may be used as another authentication measurement.³⁰

Speech is the most natural means of communication and, therefore, user acceptance of voice authentication systems is very high.³¹ However, several problems with this technique exist. A human voice can be recorded and played back, thus allowing an unauthorized user access, unless the system is set up to allow a random selection of a group of words from a larger subset.³² Voice authentication systems set up in this manner are similar to a query and response password systems. Another difficulty with voice authentication is the amount of background noise. High background noise areas are not suitable for voice recognition systems. In addition, voice recognition systems do take slightly longer to complete an authentication than many other authentication techniques.

²⁹ Naik, Jayant, M., "Speaker Verification: A Tutorial," IEEE Communications Magazine, Vol. 28, No. 1, January 1990, p. 42.

³⁰ Ibid., p. 43.

³¹ Ibid., p. 42.

³² Revillet, 1994, p. 165.

Typical voice authentication systems with quality microphones in a quiet environment can obtain high accuracy levels. By varying the acceptance threshold, it is possible to drive FAR below 0.1% while maintaining 2-3% FRR, or to obtain a FRR of less than 1% while maintaining a FAR of 5-10%.³³

2. Authentication of the Access Device

Authentication of the access device can take many forms. In its simplest form, the system checks only that the card is of the right type. Currently, the most advanced checks involve some sophisticated cryptographic challenge and response. This section reviews the more common machine authentication of access device techniques.

a. Optical Character Recognition

Optical character recognition (OCR) is a technique which allows the card reader to read *stylized* characters off the card. These characters can either be raised, as in the case of an embossed name on a card, or just printed on the card, as they are on checks. This technique provides little security, since strips of OCR printed tape, either raised or not, can be affixed to any card. This technique, has little true security application and is rather used as an automated data capture technique.

b. Magnetic Ink

Magnetic ink character recognition (MICR) is a process in which the ink used to print characters is encoded to be machine readable. This technique likewise provides

³³Naik, 1990, p. 45.

little security because it can be easily duplicated and applied to media. Magnetic ink is used mostly for automated data capture on paper items such as checks.

c. Electronically Verifiable Holograms

Electronically verifiable holograms, much like their visual counterparts, can be applied anywhere on the card. With this technique, the hologram is normally placed under the laminate of the card. With some card technologies, it is possible to place the hologram directly on the card in the area where someone would have to access in order to tamper with the card. Magnetic stripe cards are the best example of this. Holograms are being placed over the magnetic stripe, to ensure it has not been accessed and tampered with. While this technique does provide some security against tampering with the card, it does not guarantee that the magnetic stripe has not been electronically altered without access. Electronically verifiable holograms are relatively inexpensive to mass produce, and are difficult, time consuming, and expensive to duplicate. This desirable combination may have even greater application in the near future.

A related technology, called reflective particle tagging was developed at Sandia National Laboratory (SNL). This technique was developed to uniquely identify individual strategic weapons, thereby aiding in the counting of these weapons for arms control verifications. It was "designed to be secure from copying and transfer even after being left under the control of a very determined adversary for a number of years."³⁴ This technique uses tags which are composed of reflective particles suspended in an adhesive. The

³⁴Tolk, Keith M., "Random Patterns and Biometrics for Counterfeit Deterrence," CardTech/SecurTech '94 Conference Proceedings, 1994, p. 144.

reflective particles are formed by crushing a crystalline material into particles of irregular size and shape. Once suspended in the adhesive, these particles form a unique, machine readable tag which is difficult to duplicate. The reading of the tags can be accomplished in a number of ways, including cameras, and imaging processing.³⁵ This technology has not had mass appeal in card technology systems, since each tag contains a unique pattern that must be recorded for reference. However, as the cost of machine data storage capacity continues to decrease, and the need for high security card authentication increases, this technology may gain mass appeal.

d. Cryptographic Techniques

Cryptography is defined as the process of writing in or deciphering secret code. The use of secret codes dates back thousands of years, however, it was not until the first World War that sophisticated machine devices were used to perform cryptographic functions.³⁶ This section reviews the fundamentals of cryptography, introduces some of the more common cryptographic techniques, and provides examples of how cryptography can be applied to card authentication.

Figure 15 provides a block diagram of a typical encryption and decryption scheme. The scheme can work with or without a key. Systems which operate without a key, rely on keeping the nature of the algorithm secret, and are referred to as restricted. However, these systems provide inadequate security for most applications.³⁷ In systems

³⁵ Ibid.

³⁶ Schneier, Bruce, Applied Cryptography: Protocols, Algorithms, and Source Code in C, Wiley and Sons, NY, 1993, p. xi.

that use *keys*, the keys can take on any one of many values, and generally the larger the number the better. A cryptographic algorithm, also called a *cipher*, uses the key to transform the plain text into its encrypted form. These ciphers are normally mathematical functions. Encryption keys are often called public keys and decryption keys are called private keys.

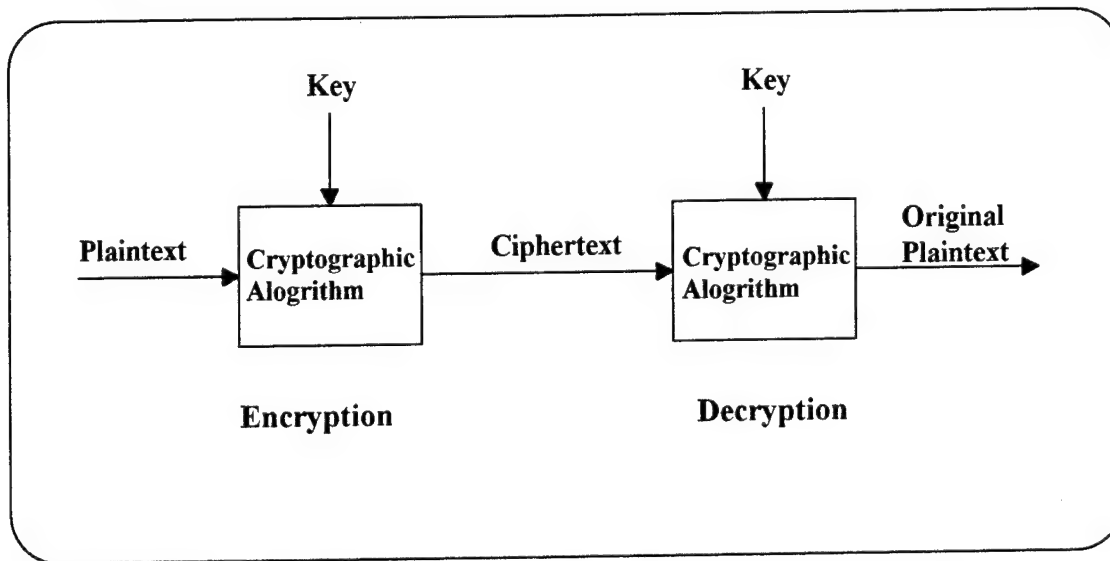


Figure 15 -- Typical Encryption and Decryption Scheme

There are also encryption schemes which only contain the first cryptographic algorithm, with or without a key, and are referred to as one-way functions. In these schemes there is no method to regenerate the original plaintext. While at first this scheme may seem useless, it is actually extensively used. Systems that compare the input authentication request to some stored reference authentication data, frequently use one-way functions to avoid maintaining a file of everyone's authentication codes. When a request

³⁷ Ibid., p. 2.

for authentication is received by the system, it performs the same one-way function on the request data, and compares the ciphertext results to the stored ciphertext reference data.

There are two major variations of systems which use both blocks and keys.

The difference is whether the two keys are the same or different. In symmetric key authentication systems, where the keys are the same, the sender and receiver must know the same key to communicate. Authentication is completed by the sending the prover an encrypted random number, if the prover can decrypt the number and return it, the prover must possess the same key, and the verifier accepts the prover's identity. In systems where there are different encryption and decryption keys, authentication is carried out by the prover generating an electronic signature with their secret key. Verifiers accept the identity of the sender, if they can decrypt the signature with the sender's public key. Since these systems require matched private and public key sets be generated by a trusted authority, key management becomes an issue, and involved key exchange protocols are frequently used.

Cryptography can be applied a number of ways to authenticate an access device. Both logic capable and memory only cards can employ cryptographic authentication, however, they do so differently. Logic capable cards can maintain the required key, and can perform interactive cryptographic functions to prove their authenticity. Both symmetric and asymmetric cryptography may be used with these cards. Logic capable cards are also capable of authenticating the card reader, and in this way can ensure against bogus information being written to the card by a non-authentic terminal.³⁸

Memory only cards, can have the data stored on them encrypted. In this manner, the cards authentication is performed by the decryption of data. If it decrypts properly, it must have been encrypted, before being stored on the card, using the appropriate key. Depending on the type of storage and encryption used, it may be possible to copy encrypted data from the card and produce forged cards. This is easily remedied with time stamps, changing bits, codes, and a host of other techniques. This technique can also be used to protect data from access by unauthorized personnel. To accomplish this, different keys can be used to store different data. In this fashion, the card reader can only access data which it has the proper key for, all other data would be unreadable.

The most common cryptographic techniques used in association with card technologies in the United States are listed below. A complete review of the operation of each system is beyond the scope of this paper, however, the references provide several sources for further information.

Symmetric Key Cryptography:	Data Encryption Standard (DES)
Asymmetric Key Cryptography:	Digital Signature Standard (DSS) and Rivest Shamir Adelman (RSA)

e. Zero-Knowledge Authentication

A final means of machine authentication of access devices, is the zero-knowledge authentication technique. This method does not use passwords, keys, or cryptographic methods for authenticating the access device. Rather, the card acceptor deduces that the access device possesses the secret accreditation by issuing one or more

³⁸Nelson, 1994, p. 48.

challenges, and the access device providing an equal number of responses. This method is relatively new, having been introduced in the late 1980s, and has not been extensively employed as yet.³⁹ However, it is known that zero-knowledge systems require a more sophisticated microprocessor, increase card cost, and further reduce memory space.⁴⁰

E. SUMMARY OF AUTHENTICATION TECHNIQUES

There is a wide variety of authentication techniques available today, and even more projected to be available in the near future. Figure 14 provided a summary of the relationships between these techniques. The selection of the authentication technique to be used in a card system, may be as important as the selection of the card technology itself.

³⁹ Ibid., p. 52.

⁴⁰ Ibid., p. 48.

V. NEW FRAMEWORK BACKGROUND

A. INTRODUCTION

The basis for the new framework presented in Chapter VI, is not only DoD doctrine, but progressive acquisition strategy as well. This chapter presents DoD support for the views adopted by the new framework, as well as several important theories and concepts used in the new framework. The first section of this chapter reviews the evolutionary acquisition concept, and relates it to card technologies. The next section discusses DoD and federal government information technology procurement strategies and directives, and how they relate to the concepts used in the framework. The final section outlines the basis for many of the theories and concepts employed within the new framework.

B. EVOLUTIONARY MIGRATION CONCEPT

The evolutionary migration concept of systems acquisition has been in use for over ten years. The Joint Logistics Commanders (JLCs) define evolutionary acquisition as "an acquisition strategy which may be used to procure a system expected to evolve during development within an approved architectural framework to achieve an overall system capability."¹ This concept is frequently applied to command, control, and communication systems, however, it is applicable to any system which is expected to evolve during its life cycle. Card technology systems are in this category. The framework presented in Chapter

¹ Hirsch, 1988, pp. 23-26.

VI, uses evolutionary migration concepts, and presents a method of selection for evolutionary card technology systems.

C. DEPARTMENT OF DEFENSE SUPPORT

The DoD and the federal government support many of the concepts which are incorporated in the new framework presented in the next chapter. This section reviews some current DoD and federal government initiatives and directives related to information technology system management and procurement.

1. National Performance Review

The Clinton administration has produced several publications dealing with reinventing government. The National Performance Review, requested by President Clinton and lead by and Vice President Gore, was established to review federal programs and identify areas for improvement. While these reports provide little substantive information on the means to achieve the discussed improvements, they do embrace many of the concepts which will be used in the new framework. Specifically, these reports support the use of life cycle cost minimization evaluations (as constrained by performance requirements), vice acquisition cost minimization.² This acknowledges the problems associated with the short-term focused, lowest bidder mentalities of many previous DoD acquisition strategies, and allows for recognition of factors other than price in defining a "best value" alternative.³ These reports also support the use of performance-based contracting.⁴ The

² Clinton, Bill J., President and Albert Gore, Jr., Vice President, Technology for America's Economic Growth, A New Direction to Build Economic Strength, February 22, 1993, p. 23.

new framework expands this concept to include performance-based target system definitions and performance-based migratory path comparison.

2. Corporate Information Management

The creation of the Corporate Information Management (CIM) initiative began in July, 1989, when the House Armed Services Committee, responding to the General Accounting Office (GAO) reports of mismanagement of automated data processing in the DoD. The GAO suggested that funding for DoD investments in Information Technology (IT) should cease until the DoD established a comprehensive strategy for its information systems which eliminated redundancy and enforced standardization. In response to Congress' suggestion, the CIM office was created in October, 1989. In the fiscal year 1991 Defense Appropriations Act, enacted October, 1990, Congress allocated one billion dollars of the Information Systems (IS) funding request directly to the CIM office, allowing them to begin implementation of CIM initiatives. These funds would be given to the requesting agencies only if the system they desired to fund met CIM requirements. The message was clear, all IT/IS proposals must have DoD wide standardization and integration capability.⁵ In July, 1991, the CIM initiative was expanded to include business

³ Gore, Albert, Vice President, Creating a Government That Works Better and Costs Less. Report of the National Performance Review, U.S. Government Printing Office, Washington, DC, September 7, 1993, p. 165.

⁴ Clinton, 1993, p. 22.

⁵ Kotheimer, William C., "A Database to Support DoD Business Process Redesign," Naval Postgraduate School Thesis, Monterey, CA, September 1992, pp. 1-2.

process redesign (BPR).⁶ BPR involves the examining of processes, and the elimination of unnecessary and redundant ones, before receiving funds to automate. This initiative also includes the combining of multiple legacy systems into single systems, and the determination of *best of breed* systems to migrate toward. An extensive application of this is being undertaken by the Defense Information Systems Agency (DISA), Center for Integration and Interoperability. DISA has identified 1271 legacy applications in 74 different functional activities that have potential for migration to common systems.⁷ The legacy applications identified by DISA are in a multitude of functional areas, including command and control, finance, health, procurement, transportation, and human resources. Many of these functions could be carried out by card technologies, and the migratory methodology followed by DISA could provide the target system definition in the first step of the new framework.

Another tool which is applied under the CIM initiative is Functional Economic Analysis (FEA). FEA is composed of two parts; functional analysis and economic analysis. Functional analysis involves analyzing what the organization does and improving processes based on this in-depth understanding. Economic analysis involves gaining an understanding of the potential value or future economic benefits of some investment.⁸ The economic analysis portion of the FEA recommends attaching performance measures to

⁶Office of Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, Director of Defense Information, Status of the Department of Defense Corporate Information Management Initiative, October 27, 1992, p. 7.

⁷DoD, Defense Information Systems Agency, DoD Information Integration Strategy Tree Diagrams, (Vol. 1), Ver. 5, March 1994, pp. i-iv.

benefits, to be able to track savings accomplishment. The new framework derives these performance measures for card technologies. FEA also discusses risk assessment, life cycle costs and the construction of *TO-BE* activities,⁹ all of which are incorporated in the new framework.

3. Command, Control, Communications, Computers and Intelligence for the Warrior

Command, Control, Communications, Computers, and Intelligence for the Warrior (C4IFTW) is a publication produced by the Joint Chiefs of Staff (JCS) and provides visionary guidance for present and future command, control, communications, computers, and intelligence (C4I) support. It envisions the migration to an integrated, interoperable battlefield C4I system, that starts with the Warrior's requirements. Although this guidance is not in the form of a structured methodology for C4I system definition, development, and acquisition, it does provide a roadmap to reach the objective.¹⁰ C4IFTW offers a considerable amount of support for concepts used within the new framework, including discussions of migratory systems in general and the migratory nature of C4I systems. It also discusses "feasibility issues such as interoperability, capacity, cost, security, and availability", and how these "can be migrated into these systems and at what cost."¹¹ Likewise,

⁸ Corporate Information Management Process Improvement Methodology for DoD Functional Managers, 2nd ed., D. Appleton Company, Inc., Fairfax, VA, 1993, p. 13.

⁹ Ibid.

¹⁰ Powell, Colin L., Gen, USA, Chairman, Joint Chiefs of Staff, C4I For the Warrior, June 12, 1992, p. 1.

¹¹ Ibid., p. 7.

it recognizes that "dramatic changes are occurring ... in the technologies that drive computing and communicating tools and techniques...."¹² C4IFTW provides a migratory path to the goal C4I architecture, similar to the method suggested in the new framework. This migratory path is complete with *waypoints*, (a concept which will be discussed within the new framework) appropriately labeled *quick fix* and *mid-term*.

4. DoD Directive 5000.1 and Instruction 5000.2

The subject of DoD Directive 5000.1 and Instruction 5000.2 is Defense Acquisition. The Directive provides a summary of acquisition policies and describes responsibilities of key officials and forums. The Instruction provides the details needed to implement the acquisition policies. Together, these two publications "establish a disciplined management approach for acquiring systems and materiel that satisfy the operational user's needs."¹³ This is accomplished through the establishment of two processes. The first is "an integrated framework for translating broadly stated mission needs into stable, affordable acquisition programs that meet the operational user's needs",¹⁴ and the second is "a rigorous, event-oriented management process for acquiring quality products that emphasizes effective acquisition planning, improved communication with users and

¹² Ibid., p. 9.

¹³ Department of Defense, "Defense Acquisition," DoD Directive 5000.1, February 23, 1991, p. 1.

¹⁴ Department of Defense, "Defense Acquisition Management Policies and Procedures," DoD Instruction 5000.2, February 23, 1991, p. 2.

aggressive risk analysis...."¹⁵ The Directive presents an integrated management framework (IMF) "intended to provide the basis for developing and publishing acquisition management policies ... that are consistent with and support the requirements generation system ... described herein."¹⁶ The IMF has an in-depth requirements generation system that produces information for decision makers on projected mission needs. The IMF supports the evolutionary approach to system acquisition and enjoins "decision makers to make cost-performance-schedule trade-offs at critical points in the program's implementation."¹⁷ The mission needs generation phase of the IMF is similar in concept to target system definition portion of the new framework presented in the next chapter. The cost- performance-schedule trade-offs in the new framework further capture the time preference aspect for performance, and make these decisions more apparent. The new framework leads the decision maker from broad needs, to functions, to technical capabilities required for support of these functions. In contrast, the IMF goes from broad needs, to performance objectives, to system-specific requirements. While this may be useful for static systems acquisition, it is much more difficult to apply to evolutionary systems.

5. Technical Architecture for Information Management

The DoD Technical Architecture Framework for Information Management (TAFIM) is a draft, eight volume publication produced by the Defense Information

¹⁵ Ibid.

¹⁶ DoD Directive 5000.1, 1991, p. 3.

¹⁷ Ibid.

Systems Agency (DISA), Center for Architecture. This publication is intended to be the means for DoD to achieve its Information Technology (IT) and Information Management (IM) goals. Whereas the C4IFTW and CIM initiatives provided the **vision** of where DoD should be going in terms of information technology management (ITM), TAFIM provides the **plan** of how to get there. To this end, TAFIM provides guidance in several areas, including architecture concepts, design, acquisition, security, standards, and human computer interface of IT and IM products. TAFIM also offers two methodologies; the Technical Reference Model (TRM) providing the conceptual model for information system services and their interfaces, and the Standards-Based Architecture (SBA) Planning Methodology. TAFIM volume four presents the seven step SBA planning process, which leads the user from project initiation through implementation and administration. For each step, TAFIM provides an in-depth discussion of the objectives, scope, deliverables, critical success factors, constraints, task list, effectiveness measures, and completion criteria, as well as required tools and staffing skills.

While this draft SBA provides excellent detail on accomplishment of steps toward a new system, the SBA methodology has some flaws. Noticeably, the temporal component of these systems is neglected. The new framework, presented in the next chapter, is an alternative methodology to the one presented in TAFIM. Much of the supporting guidance presented in TAFIM is applicable to the new framework as well and will not be reiterated within the new framework.

D. THEORIES AND CONCEPTS

The new framework incorporates several theories and concepts. While these are not controversial in nature, a presentation and discussion of each is appropriate background at this point. There are other basic concepts which could be discussed before presentation of the new framework, however, the reader is expected to be familiar with most of these concepts. The few concepts which are presented here, are presented for completeness, and to ensure reader/author commonality of terminology and concept application.

1. Analytical Hierarchy Process

The Analytical Hierarchy Process (AHP) was developed by Thomas L. Saaty and is designed to solve complex problems involving multiple criteria. The process can be used to create values for both the relative importance of decision criteria and the relative preferences between alternatives within these decision criteria. AHP is used in the new framework in both of these roles. It is used to weigh the relative importance of the various measures of performance, as well as to weigh the relative ability of each migratory system in these performance measures.

AHP was chosen for a number of reasons. The comparison of a finite set of performance measures and migratory path options lends itself well to AHP's pair-wise comparison of items, and is relatively easy to apply. Although there has been much discussion of the problems with the accuracy in AHP weights,¹⁸ it does produce reasonable information for which to base decisions on. Given the relative inaccuracies of other parts

¹⁸Dyer, James, Thomas Saaty, Patrick Harker, and Luis Vargas, "Discussion of AHP", Management Science, Vol. 36, No. 3, March 1990, pp. 247-275.

of the framework, such as future cost estimations, economic forecasting, and performance measures, the AHP estimations are judged by the author not to be a significant source of error. However, other analysts may conclude other weighting schemes, such as SMART, are more appropriate, or may opt to use an alternate method. Alternate methods include multi-attribute utility theory (MAUT), goal programming, utility theory, and others.

2. Commercial-off-the-Shelf

Commercial-off-the-shelf (COTS) is a term used to define products, systems, system components, software, etc., which are available for sale publicly. The opposite of this, are products which are produced solely for the government. There has been much attention to the purchase of COTS products verses the development of application specific items for significant costs savings. The new framework could be applied to either COTS or developmental applications. Smart card technologies are well vendor supported at this point, and most procurement will be of COTS products. Likewise, databases to store card system data could contain minimum developmental effort and utilize as much COTS products as possible.

Related to COTS, is Government-off-the-shelf (GOTS), which are products which have been developed for government use, and are readily available to government agencies. To the government consumer, these items are similar to COTS products, but may be available at substantial savings.

Although not captured within the new framework itself, the decision to use a COTS or GOTS product verses a full development effort effects many aspects of the new

framework. The costs associated with a development effort would be considerably more, and would be substantially different in composition. The new framework, although it could be applied to a development problem, is geared toward COTS or GOTS product acquisition.

3. Open Architecture

Open architecture is likewise not captured within the new framework, however it is an important decision. Open architecture systems allow the product to be integrated with products of other manufacturers. Open architecture provides a standardized means of conducting functions such as data transfer, database access, card access, storage, and the like. In contrast, proprietary systems are ones belonging to a specific manufacturer, and are not compatible with other systems. Selecting proprietary systems limits the choices, especially for future migratory upgrades, to a specific product line.

4. Discounting to Obtain Present Values

Within the new framework, the concept of discounting to obtain present values is applied to the future expenditures estimated in the cost model. Since many of the expenditures in a migratory system will be delayed for many years, the discounting of these costs plays an important role in final migratory path selection. The reader is assumed to be aware that time effects the value of money. Therefore, this section describes discounting application, but not the theory and reasoning behind discounting.

To obtain the present value (PV) of a future cost, the PV discounting formula is used. This formula is given as Equation 3.

$$PV = F_n * (1/((1 + i)^n)) \quad (3)$$

where: F_n = future cost in period n
 i = period interest rate
 n = number of periods

This formula can be applied to any period definition, such as months, quarters, years, etc., as long as the interest rate per period is used. This allows for simplified calculations within the framework, by aligning this with the period used for the measures of performance calculations. Determination of the appropriate interest rate to use is a more difficult problem. Ideally, the interest rate used should be the weighted average opportunity costs of the money to be used. This is difficult to estimate, since these costs are in the future and therefore the interest rate is a future interest rate. While it is possible to use different interest rates for different periods, based on economic forecasting, this is rarely done. Rather, the formula provided above is used, incorporating an average interest rate for the time period.

The government makes this choice somewhat easier. The DoD requires the use of an interest rate of ten percent be used on all project costs and benefits that go over three years from project inception date. This figure is designed to represent the weighted average opportunity cost of taking money from the private sector (the source of government funds). It also provides a common basis for economic analysis and prevents the altering of the interest rate to make one project look better than another.¹⁹

¹⁹Haga, William, J., and Robert Lang, "Revised Economic Analysis Procedures for

5. Cost Analysis Concepts

Cost analysis is an art unto itself, and an in-depth discussion of this topic is beyond the scope of this thesis. However, to apply the new framework, the decision maker must be able to obtain reliable, pertinent cost information for the alternate migratory paths. Cost data for currently available technology is relatively easy to obtain from vendors, contractors, other installations using the technology, trade publications, trade conferences, and the like.

However, forecasting expected costs for technology some time in the future is difficult. What is expensive today and looks to remain expensive, may become reasonable through a number of means such as a scientific breakthrough, or a new use for the technology which drives volume up and price down. The opposite is less often the case, but it is possible to have the costs of technology unexpectedly rise through natural disasters, increased demand without increased availability, or other factors.

6. Risk Analysis Concepts

As discussed in Chapter II, risk analysis is a context dependent concept. Risk analysis is a technique to identify, characterize, quantify, and evaluate the hazards of a project.²⁰ Security risk analysis, assesses the security risks involved in the project, and determines the required amount of security needed. Technological risk assessment, assesses

ADP," Naval Postgraduate School Manual, Monterey, CA, January 1991, pp. 8-1 through 10-20.

²⁰ Modarres, M., What Every Engineer Should Know About Reliability and Risk Analysis, Marcel Dekker, Inc., NY, NY, 1992, p. 297.

the effects of future technologies not reaching expected levels. Economic risk assessment, assesses the effects of economic changes on project completion.

Risk assessment involves two distinct steps: A qualitative identification, characterizing, and ranking of the hazards; and a quantitative estimation of the likelihood, and consequence of the occurrence of each. The *risk level* is the sum of the likelihood and consequence of occurrence of each undesirable event. Risk levels are most useful when consequences can be measured in financial or other measurable terms. In the new framework, risk analysis is used to determine the likelihood of each migration path occurrence. The likelihood of occurrence is multiplied by the overall net value of the path, to determine net expected value of the path. Used in this manner, the risk assessment takes into account economic and technical risks. Risk assessment, much like cost analysis, involves estimates and future predictions, and is an art form. There are inaccuracies involved with any technique that involves estimations and future predictions, however, a properly conducted risk analysis can provide reasonable estimates of likelihood and consequence of occurrence.

E. SUMMARY

This chapter presented the basis for many of the concepts used within the new framework. It is not intended to be an exhaustive discussion nor an instructional aid to each concept, however, it should provide the user with the necessary background and references to apply the new framework.

VI. A FRAMEWORK FOR CARD SYSTEM SELECTION

A. INTRODUCTION

1. Framework Purpose and Problem Statement

The purpose of this chapter is to present a new framework for evaluating evolutionary upgrade paths for card systems. As already discussed, card system procurement is evolutionary in nature, as these systems will go through many changes during their useful life. As emerging technologies mature, the system will be incrementally upgraded. System procurement alternatives that capture this temporal component are evolutionary upgrade paths to some future goal or target system.

The framework presented here is a functionally-oriented, capability-based approach. It is intended to be a step-by-step method which produces information useful to the decision maker about alternate evolutionary upgrade paths.¹ The problem answered by the new framework is maximize "utility of life cycle performance" less "utility of life cycle cost," subject to technological (physical and human competence) feasibility, target functions and capabilities, and current systems and their capabilities. The required target functions and capabilities are a constraint to make the framework a cost-performance tradeoff with explicit consideration of the time preference for when the target functionality will occur. This simplifies the "real" problem by fixing the target time (the end of the

¹ Egge, Daniel, Q., "A Framework For Evaluating Evolutionary Upgrade Paths of Command, Control and Communications Systems," Naval Postgraduate School Thesis, Monterey, CA, June 1993, p. 38.

planning period) when all the target functions and capabilities must be obtained. The two variables, utility of life cycle performance and utility of life cycle cost, are not directly measurable. However, within the framework, a figure for the utility of life cycle performance will be developed using a measure of performance hierarchy and performance attribute scales. Life cycle costs will be estimated using standard cost analysis tools. These two figures will then be scaled to be of the same magnitude, and now being in the same measurement units, can be subtracted from each other. In this fashion, the framework is able to capture the entire life cycle cost and performance figures, including evolutionary upgrades, and not just initial procurement, operation and performance estimations. It also encompasses technological feasibility issues and system reuse, including data and human capital, as well as hardware and software.

2. The Need for an Effective Evaluation Framework

As was noted in Chapter II, there are many issues which must be considered in the selection of a card technology system. This new framework captures the 12 categories of issues presented in Chapter II, and aids the decision maker(s) in making conscious decisions about alternatives, including the placing of weights on their choices. Chapter II categories 1 through 8, the performance issues, are incorporated into the measure of performance calculations performed in the third step of the new framework. Category 9, system life expectancy, is required to be considered as part of the first step in the framework. Category 10, cost estimation, is captured in the cost estimations made as part of the fourth step of the framework. Category 11, risk assessment, is captured in the risk

weights required to be applied to each migratory path in step six of the framework. Category 12, the temporal component, is addressed in the time preference weights given to the measures of performance by the decision maker in step three.

3. Methodology

The framework is presented as a step by step procedure, along with some illustrative examples of step application, and comments on step accomplishment. The framework presented is geared toward card system procurement, however it could be applied to any evolutionary system acquisition. The reader is assumed to have a level of knowledge about procurement, cost estimation, system benefit analysis, and other concepts. Where appropriate, footnotes are provided so that additional in-depth information on the topic may be located.

B. THE FRAMEWORK

1. General Discussion

Before the steps in the framework are presented, a general discussion of the framework assumptions is appropriate. The problem of card technology system acquisition could be approached in a number of ways. The goal could be defined in one of three ways; getting a set level of performance for a minimum life cycle cost, getting maximum performance for a set cost, or some form of cost-benefit tradeoff. The set cost problem is not representative of typical DoD procurement. The evolutionary nature of card technology systems make evaluation by conventional cost-benefit analysis difficult. The new

framework provides a cost-benefit scheme which captures the temporal component. Figure 16 provides a graphical view of cost-benefit tradeoff decision.

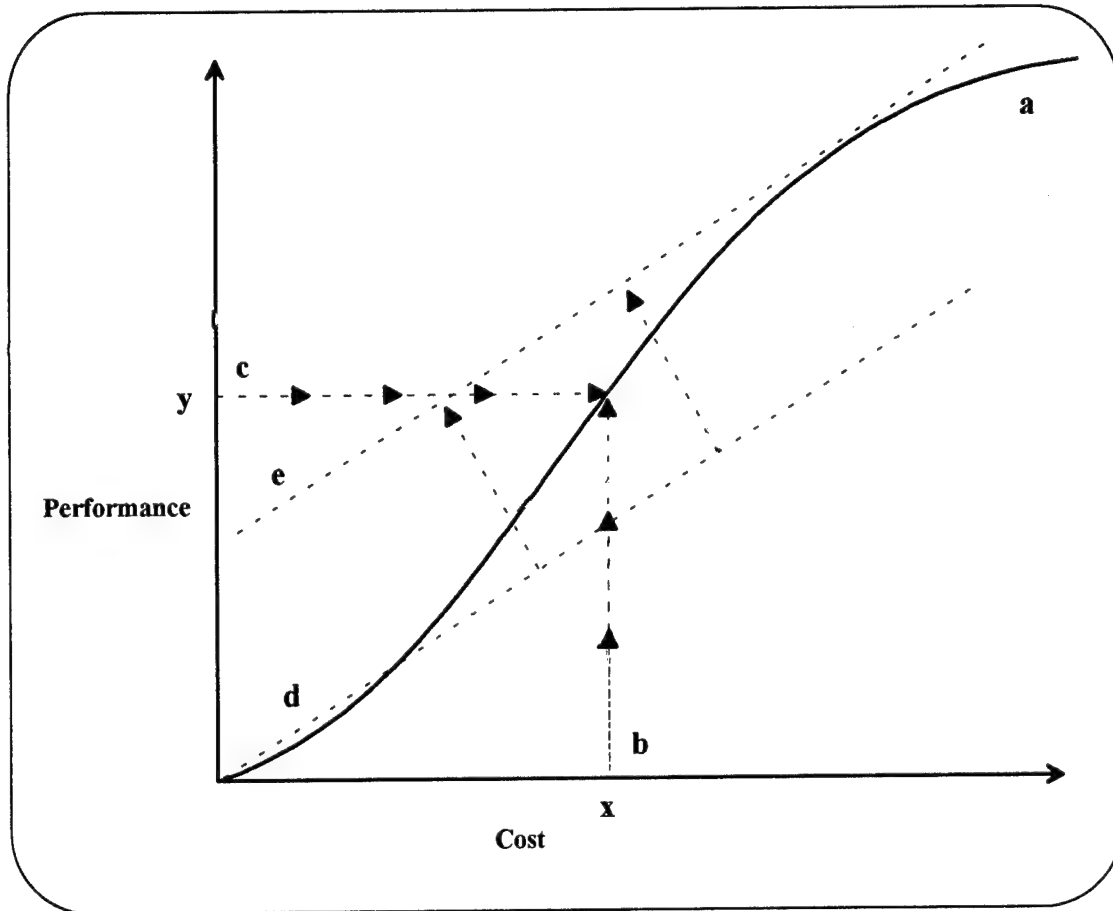


Figure 16 -- Cost Performance Decision Curve

Line **a** is the performance-cost curve for a card technology. It also represents the present limit of technological feasibility. Line **b** is the intersection point on the cost-performance curve, given a cost limit of **x**. Line **c** is the intersection point on the cost-performance curve, given a performance level required of **y**. Line **d** has a slope equal to the preference for performance versus cost, and is drawn through the origin. To obtain

the optimal cost-benefit tradeoff solution geometrically, line **d** is shifted in a parallel manner to the point at which it is tangent to the performance-cost curve. That is, the point of tangency is the best combination of cost and performance (as represented in the slope as the explicit tradeoff of cost and performance) that is technically feasible. Line **e** in Figure 16, is line **d** shifted to be tangent to the cost performance curve.

The new framework allows the cost-performance trade-off to capture the temporal nature of the acquisition problem. This allows the user of the framework to maximize life cycle performance less cost, while achieving the level of performance at a specific time that is preferred. In order to accomplish this, several issues must be resolved including how the set level of performance is defined, when the level of performance will be achieved, the time weighted value of the migratory system performance capabilities, the likelihood of being able to achieve this level of performance, and others. These questions will be answered within the confines of the framework. The problem answered by the new framework is maximize "life cycle performance" less "life cycle cost", subject to technological feasibility, and current systems and their capabilities.

The framework will complete calculations based on a breakdown of the useful life of the system into time periods. The length of these time periods is at the discretion of the user. However, a few guidelines should be followed. The time periods should not be too short, as this will cause the number of calculations, estimations, and weights to become unmanageable. Likewise, time periods should not be too long, as this will cause cost estimations, discounting, and weighting to be less accurate, due for example to

technological change and economic change. For the illustrative examples provided, the assumed ten year useful life is broken down into ten, one year time periods.

2. Overall Framework View

The framework contains seven top level steps, each containing one or more sub-steps. These seven steps are:

1. Define the target and current systems, in terms of functions, capabilities, and useful life.
2. Determine viable migratory paths from current or base systems to the target system.
3. Develop and weigh the multiple measures of performance (MOP) for the card system, and calculate an overall MOP for each migration path, using the Analytical Hierarchy Process (AHP).
4. Develop a hierarchical cost model for the card system, and calculate an overall life cycle cost for each migration path.
5. Develop a preference for cost and performance, and use it to calculate an overall net value for each migration path.
6. Develop a likelihood of occurrence for each migration path and select the migration path with the greatest expected value.
7. Reevaluate and return to step one.

Figure 17 provides a graphical summary of the steps in the new framework. The graphic representation of the framework shows the sequence of steps, as well as the recursive nature of the framework. Steps three and four can be completed concurrently, however, they must be completed prior to step five. This overall view will be used to illustrate each of the steps throughout the new framework.

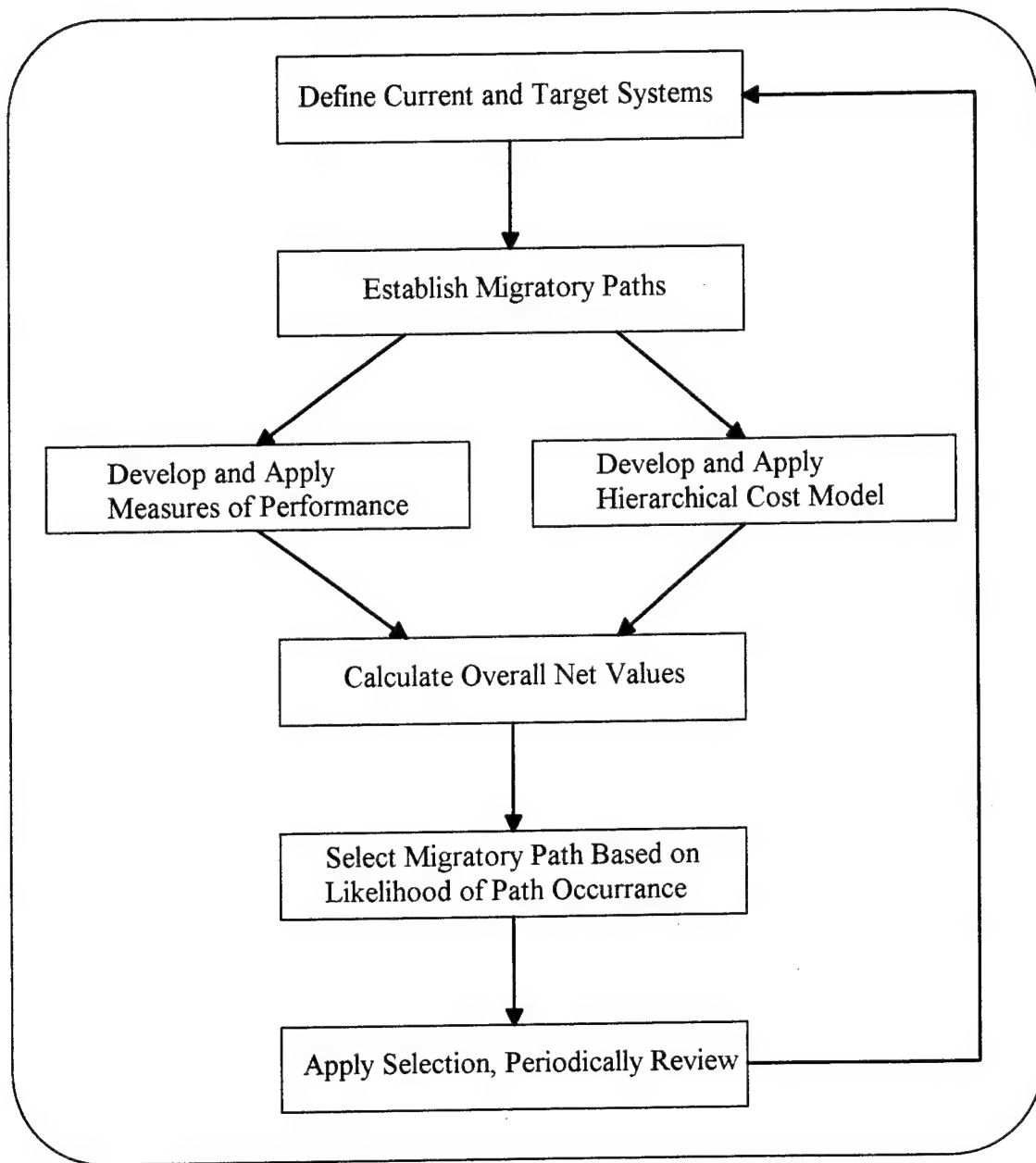


Figure 17 -- The Steps of the New Framework

3. Framework Steps

a. *Define Current and Target Systems*

The first step in the framework is the definition of the current and target systems. Figure 18 summarizes this step. This step involves determining what functions are desired in the system that will eventually be, as well as what technological abilities the card

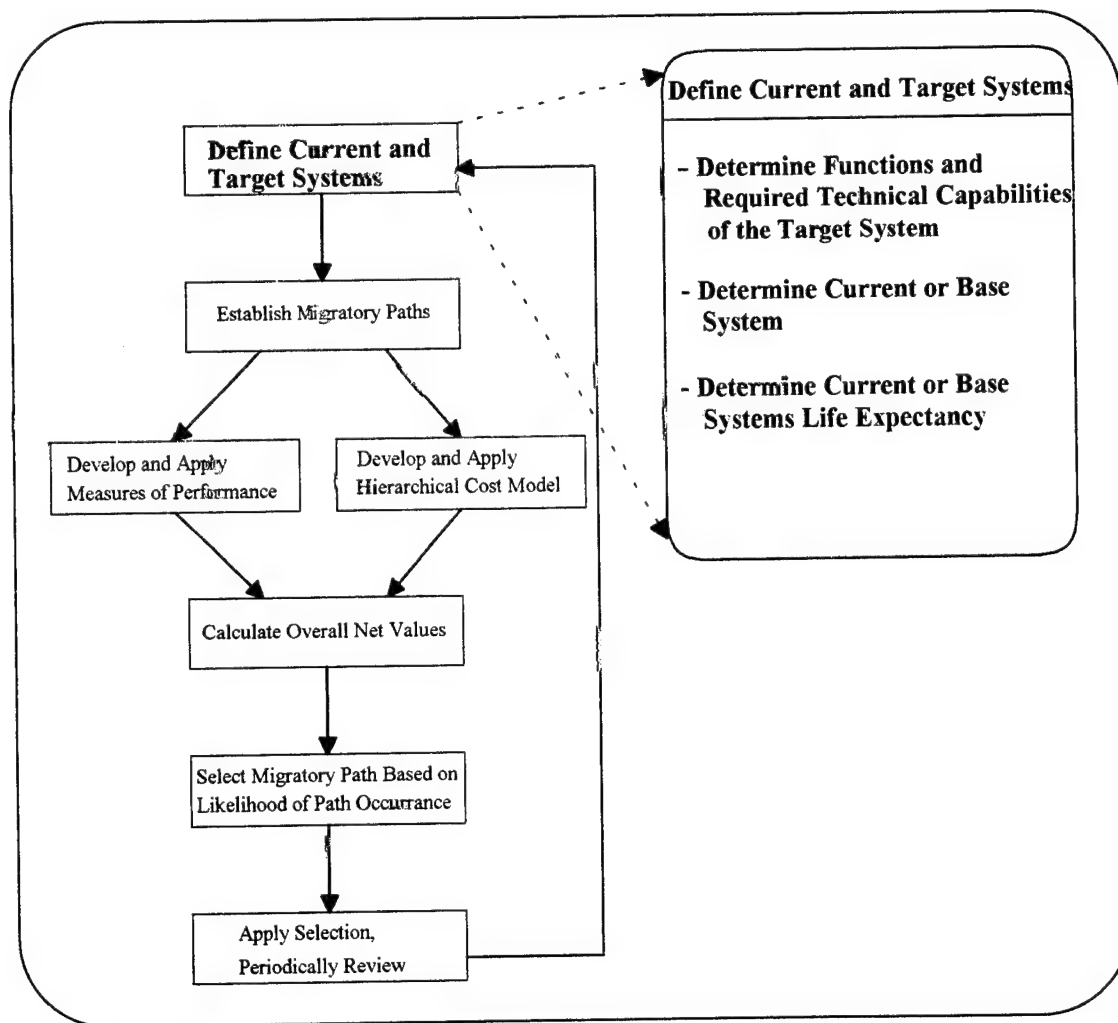


Figure 18 -- The New Framework - Step 1: Define Current and Target Systems

system must have in order to fill these functions. In addition, the decision maker must clearly define the base or current system. The target system definition must be based on a thorough review of needs. How this is accomplished is left to the user, however, there is considerable literature and DoD support for the development of mission needs statements, as well as total quality leadership guidance on reengineering processes. Whatever the system used, the end product should be a clearly defined target system definition. This step also requires the decision maker to determine the life expectancy of the current system.

(1) Determine Functions and Technical Capabilities. The target system must be clearly defined at the outset of the evaluation. This in effect sets the level of performance at the end of the planning horizon. Without a clearly defined target, it is impossible to complete the cost-benefit analysis. The target system is one which provides the anticipated level of functionality desired of the card system at some future point. To define this target system, a functionality versus technical capability table should be constructed. Each desired target system functionality will require the system to have one or more technical capabilities. Table 2 provides a sample card technology versus technical capability table. The table can be filled in using X's as required capabilities and O's as optional capabilities to support the function, or with numbers relating to the level of technical capability required (levels are discussed further under Step 3 and Appendix C), or with low (-), medium (*), high (+) indications. There has been work done on functionality versus technological capability tables for card technologies, and this work was used to create this table.²

²Bower, Leslie, "Automated Data Card Technologies: The Development of Functionality and Application Matrices," Naval Postgraduate School Thesis, September 1994.

TABLE 2 -- SAMPLE FUNCTIONALITY VERSUS TECHNICAL CAPABILITY

Function	S t o r e M o n e t a r y V a l u e	S e c u r e D a t a S t o r a g e	B i o m e t r i c A u t h e n t i c a t i o n	H a n d s F r e e O p e r a t i o n	A c c e s s C o n t r o l	A u t o m a t i c D a t a C a p t u r e	C r y p t o g r a p h i c C a p a b l e	M e d i c a l R e c o r d S t o r a g e	D a t a T r a n s f e r i n E M I	E l e c t r o n i c C e r t i f i c a t i o n	E l e c t r o n i c B e n e f i t X f e r	I n v e n t o r y C o n t r o l	T i m e / A t t e n d a n c e T r a c k i n g	L o g i s t i c s C o n t r o l
Technical Capability														
Memory Capacity	*	+	-				*	+		*	*	*		*
Logic Capability	X						X			X	X			
Card Data Security	+	+	+		*	-	+	*		+	+			
Error Detection	+		+		*		+		+	+	+	*		*
Passive Operation			O	O	O	O		O	O			O		O
Interactive Operation	X	X	O	O	O	O	X	O	O	X	X	O		O
Contactless Operation				X								O		O
EMI Resistant									X					
Data Transfer Rate	-						*	+		*				
Data Transfer Distance	-			+								+		+

(2) Determine Current and Base System. The current system is easily defined as those systems that are currently carrying out some or all of the functions which are to be automated through the use of a card technology. If no system is currently in use, or if

no reuse of the current system is possible, then base systems must be used. Base systems are those systems which can be purchased in the near term to automate some subset of the functions listed in the target system's functionality/technical capability table. All potential base systems which can be reasonably expected to someday obtain the level of functionality desired in the target system, should be defined as alternate base systems. Base card systems are discrete alternatives, and can include any of the card technologies presented in Chapter III.

(3) Determine Life Expectancy of Current or Base System. To apply the evolutionary framework, a reasonable planning horizon must be selected, to provide the upper bounds for the calculations of cost and performance. The card system analysis planning horizon used should be the same as the planning horizon used by the entity as a whole. What planning horizon an entity should use has many factors to it, including the ability to forecast, and interest rates, and is beyond the scope of this thesis. The planning horizon of the organization may be longer or shorter than the life expectancy of the card system to be procured. If it is shorter, follow on card systems must be included in the evaluation to bring life expectancy equal to or greater than the organization's planning horizon. If the life expectancy of the system is greater than the planning horizon, some valuation of scrap or residual value at the end of the planning horizon must be made. If this is not possible, then a list of available assets, human knowledge, as well as physical is made. The life expectancy is usually limited by the life expectancy of major system hardware components. With card technology systems, the major hardware item used is the card reader or

acceptor device. Since these card readers are mechanical devices, a life expectancy is fairly easy to determine. Data on the mean time to failure (MTF) for the various card readers are available from both manufacturers and independent testing agencies. In the illustrative examples given in this chapter, a ten year planning horizon will be assumed.

b. Establish Migratory Paths

Once the target system, base or current system, and life expectancy have been determined, the next step is the establishment of potential migratory paths (MPs) from the base systems to the target system. Figure 19 summarizes this step.

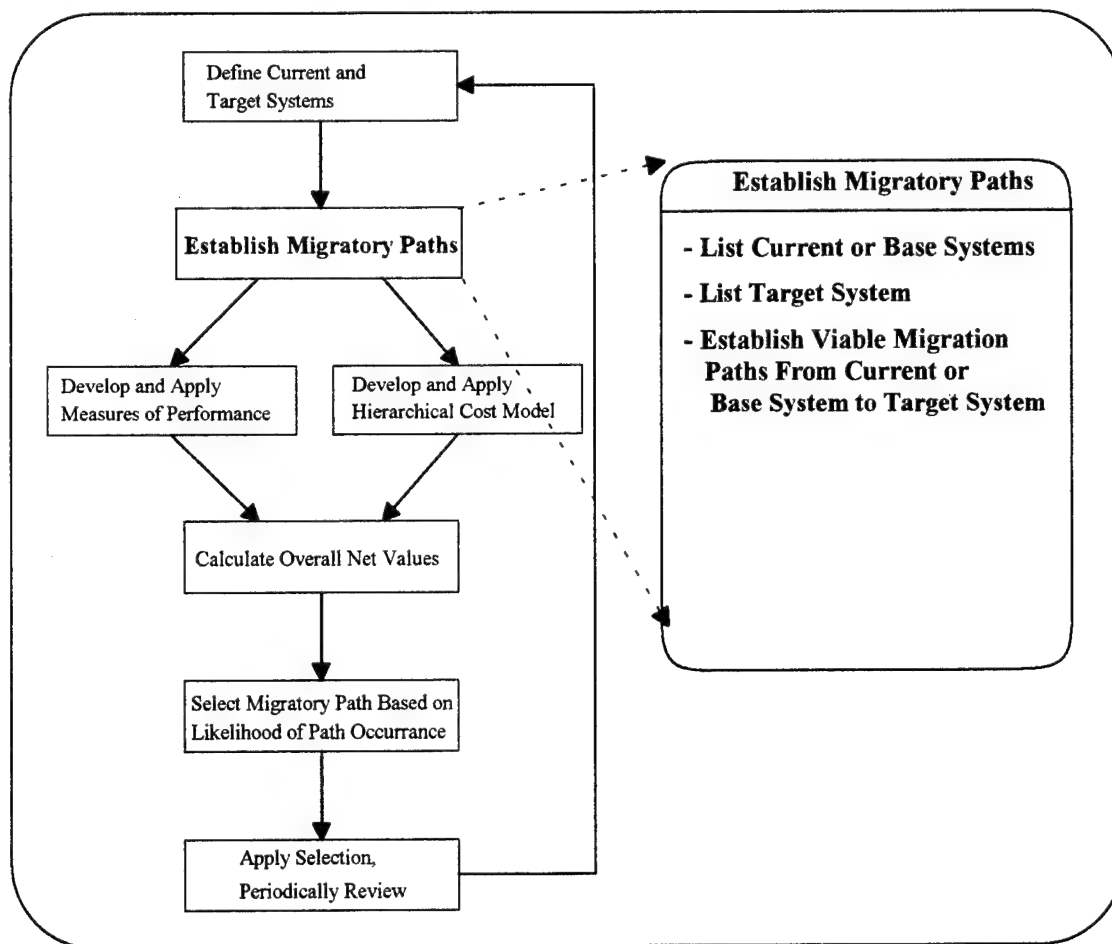


Figure 19 -- The New Framework - Step 2: Establish Migratory Paths

(1) List Current or Base Systems. The first sub-step is to identify assets and systems being used to currently carry out the functions to be automated. From this identification of assets, some reuse may be possible. As was discussed earlier, current or base systems may already be in place, may already be procured but not yet in place, or may not have been procured yet, but available in the near term.

(2) List Target System Attributes. From the target system functionality and required technological capabilities identified in step one, a clear picture of the target system's attributes can be established. The form of this target system attribute list is unimportant, as long as the decision maker(s) have a clear vision of the target system they desire to migrate toward.

(3) Construct Viable Paths to Target System. The construction of these migration paths require considerable analysis. Migration paths represent all of the possible paths by which the user could get from the current or base system to the target system. Each of these migration paths may be a different technology, or may be the same technology applied differently. The construction of migratory paths can use several sources for information. Expert consultants in the field of card technology can be used to provide information on future technology and migration path alternatives. Vendors of card technologies can also provide data of future upgrades expected in technology technology. Trade shows, such as the CardTech/SecurTech conference held in the spring in Washington, D.C., are also excellent sources of information. Unfortunately, there are few books on the subject. The CardTech/SecurTech conference proceedings are a useful source.

Because the target system may have some functionality which is not currently available, the establishment of these migration paths frequently involve technological forecasting. Figure 20 shows the relationship between current or base systems, target systems, and possible migratory paths. Curves A, B, C, D, and E are migration paths from the current or base system to the target system. Migration path E also shows two waypoints M and N. Waypoints are major milestones in the system's life cycle. They can be major system changes, integration of major legacy systems into the new system, required technological advances, or any other intermediate goal on the way to the target system. These waypoints effectively break the migration path down into manageable shorter term goals.

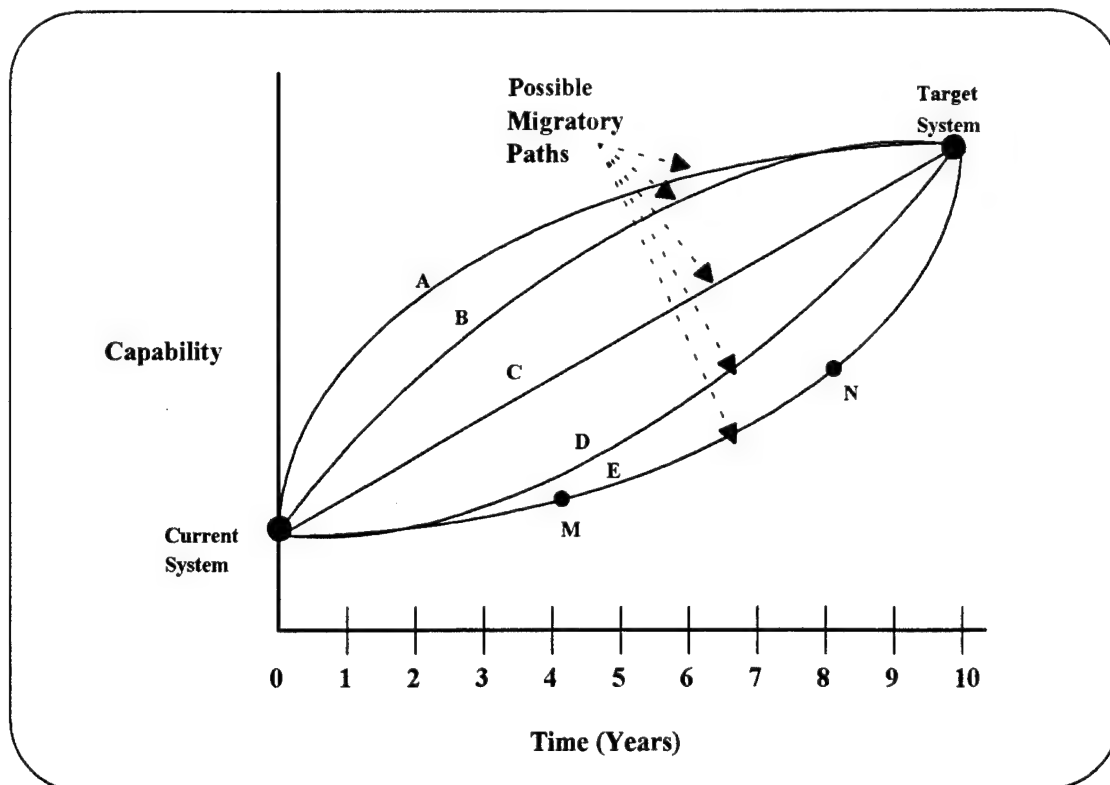


Figure 20 -- Migration Paths

c. Develop and Apply Measures of Performance

The third step in the new framework is to develop and apply measures of performance to the target system and migratory paths established in steps one and two.

Figure 21 summarizes this step. This step has several sub-steps, each of which is discussed below.

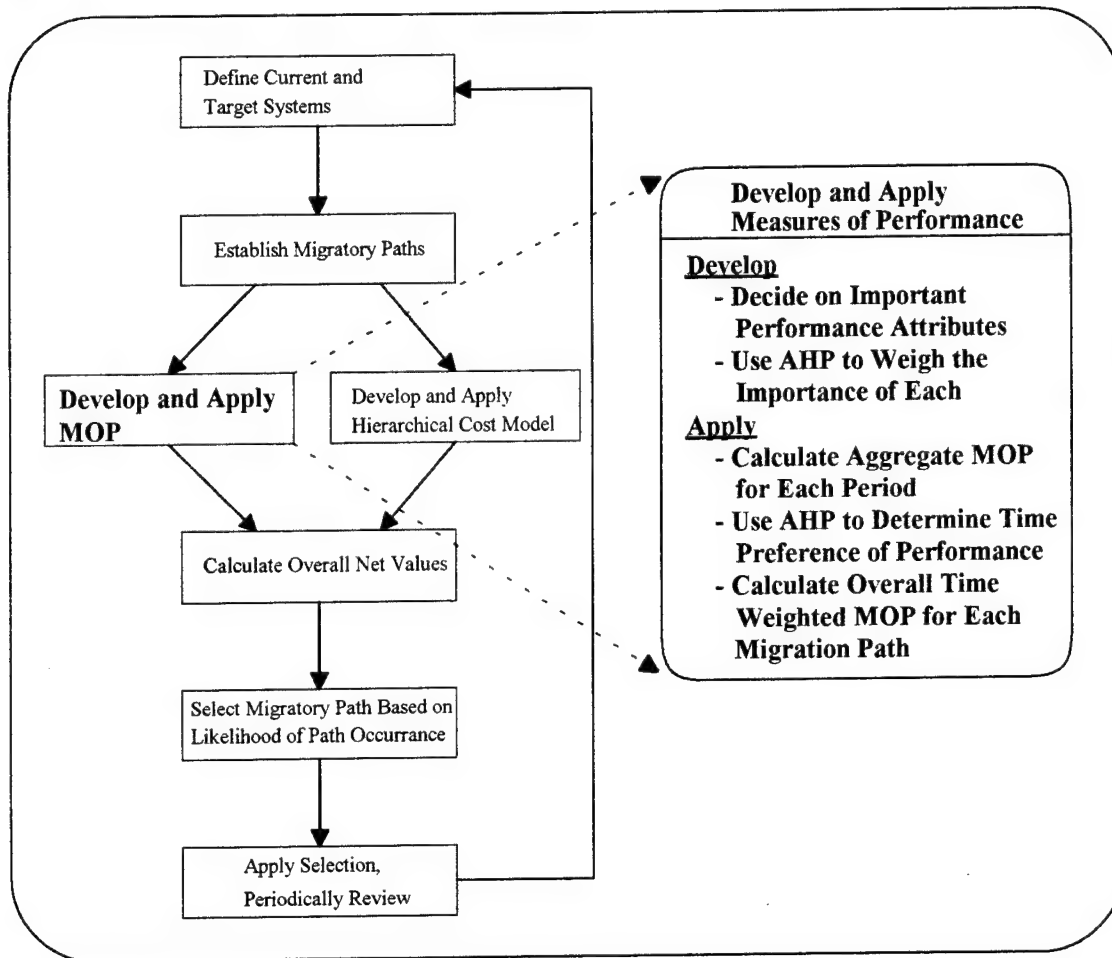


Figure 21 -- The New Framework - Step 3: Develop and Apply MOP

(1) Determine Performance Attributes and Scales. Before measures of performance can be determined for the various migration paths, a list of performance

attributes that will be used to evaluate the systems must be generated. The list of performance attributes to be used should be as comprehensive as possible, and at this point the user should not be concerned with how performance will be measured, how important the performance attribute is, or any other application concern. The goal of the first part of this sub-step is to produce a comprehensive list of performance attributes.

Once the list of performance attributes is established, it is helpful to graphically represent it in hierarchy form. This allows the grouping of some of the finer performance attributes into larger categories. Figure 22 provides a sample measure of performance hierarchy. The user of this framework may generate their own MOP hierarchy, or may apply the provided one to their problem. The reader will notice the category labeled *Application Specific MOP*, provided as a convenient place to add performance measures unique to their problem.

The final part of this sub-step is to determine a scale for each of the major categories of performance. The scale provides an indication of the possible range of the performance attributes. The scale should range from currently available, inexpensive capabilities to not yet available, visionary capabilities. These scales may be linear or logarithmic and may use any number of entries. As can be seen in Figure 22, each of the measure of performance categories can be broken down into multiple components. These components are the major determinants of that category's performance. A sample scale, for the performance attribute *Interface Robustness* is provided below. A linear, 1-10 scale was determined to be most appropriate for this category. As shown in Figure 22, the

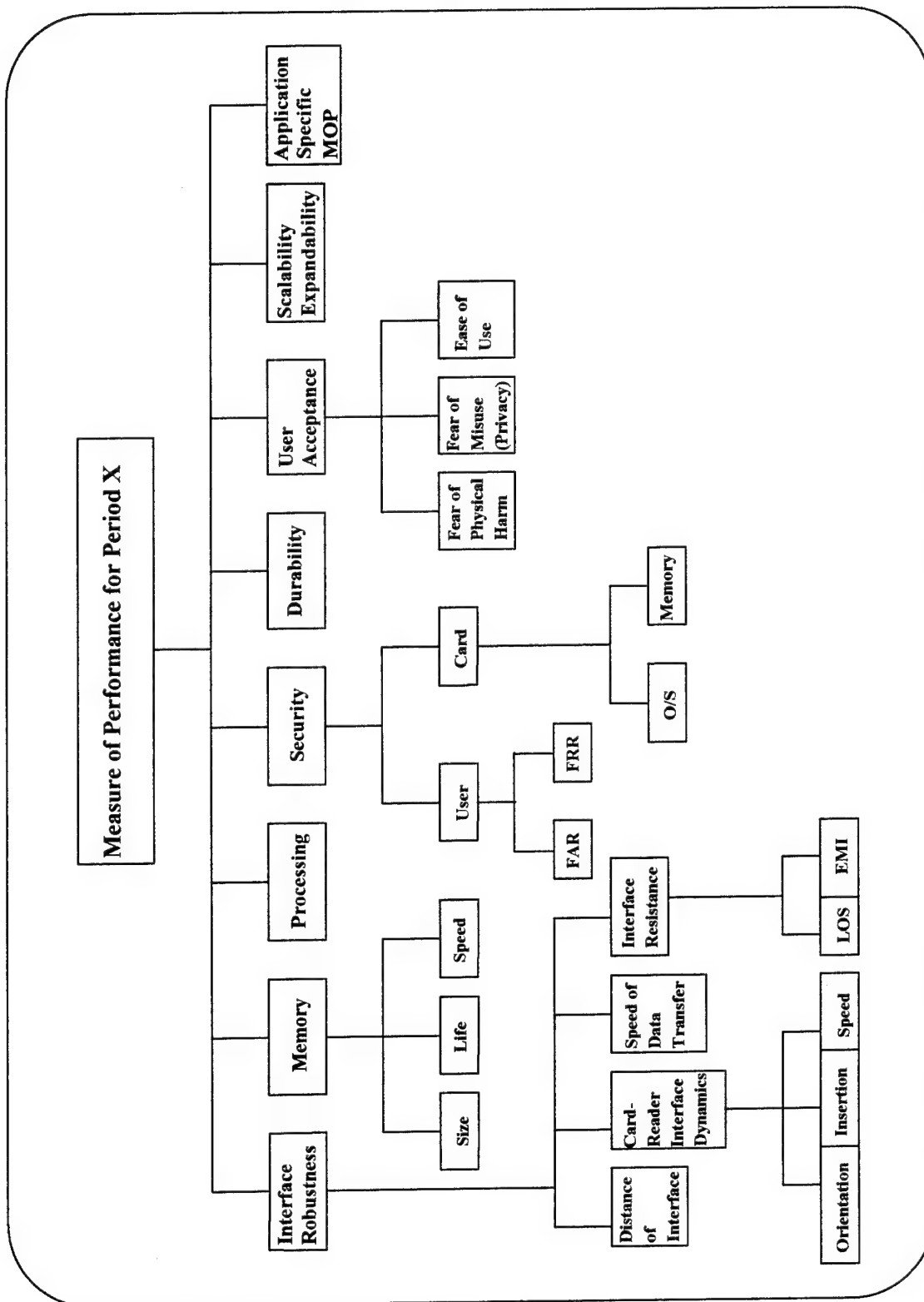


Figure 22 -- Measures of Performance Hierarchy

major determinants the robustness of the interface between the card and reader are: Distance of interface, speed of data transfer, card insertion or orientation requirements or speed of travel allowances, line of sight requirements, and electro-magnetic interference (EMI) resistance.

Interface Robustness Scale:

- 1 - Contact interface, slow data transfer rates, insertion, EMI resistant (e.g., contact ICC)
- 2 - Contact interface, high data transfer rates, insertion, EMI resistant (e.g., optical memory cards)
- 3 - Slot operation contactless, low data transfer rates, requires card orientation (e.g., Wiegand, Bar Code)
- 4 - Proximity, low data transfer rates, requires card orientation, non-EMI resistant, LOS required (e.g. inductively powered proximity)
- 5 - Proximity, low data transfer rates, no card orientation, non-EMI resistant, LOS required (e.g., battery powered proximity)
- 6 - Few to several feet, medium data transfer rates, low speed of card travel, non-EMI resistant, LOS required (e.g., battery powered radio frequency card)
- 7 - Several feet, medium data transfer rate, medium speed of card travel, non-EMI resistant, LOS required (in development)
- 8 - Few Feet, high rate of data transfer, high speed of card travel, EMI resistant, LOS required (not available presently)
- 9 - Tens of feet, high rate of data transfer, high speed of card travel, EMI resistant, LOS required (not available presently)
- 10 - Tens of feet, high rate of transfer, high speed of card travel, EMI resistant, no LOS requirement (not available presently)

Similar scales for the other non-measurable attributes could be developed. A performance scale for more measurable attributes, such as memory capacity, could be placed on a logarithmic scale of amount of bytes of data. Sample scales for some of these attributes are included in Appendix C.

(2) Use AHP to Develop an Aggregate Measure of Performance (MOP).

Once the measure of performance scales have been developed, the next step is to weigh the importance of each of the measures of performance. While this could be done a number of ways, AHP was determined, by the author, to be the most appropriate. Using the AHP's pairwise comparisons, a relative weight of the importance of each category can be obtained. While it would be possible to use AHP to weigh each of the performance attributes identified, doing so could become extremely involved. If that were done, then the weighting of the individual performance attribute would be the sum of the weights of the categories it is in. For example, in the sample MOP hierarchy in Figure 22, if the Security category were weighted 0.4, and the Card, User, FAR, and FRR sub-categories each weighted 0.5, then the Weight for FRR by itself would be $0.4 \times 0.5 \times 0.5 = 0.1$.

(3) Calculate the Aggregate MOP for Each Period. Once the MOP weights have been established for the categories, the aggregate MOP for each time period in the useful life of the system must be calculated. This is accomplished by multiplying the category scale achieved by the system during that period by the weight for that category. In this manner, the user calculates an aggregate MOP for each period in the useful life.

(4) Use AHP to Develop the Time Preference of Performance. The next sub-step in this step is to determine the time preference for the aggregate MOP. Again, AHP was chosen for consistency and ease of use. An AHP pairwise comparison of each of the periods in the useful life of the system are compared in order to determine the weighting for each period. A word of caution is appropriate here. In order to simplify the problem into a linear one, the new framework has the user only weigh the time preference for the entire measure of performance. While it is possible to time preference weigh each of the individual categories of performance, or even each of the individual MOP elements, this would greatly complicate the problem and make it non-linear. While this is a limitation of the framework, it greatly simplifies the problem, and is deemed by the author not to be a significant source of error, in light of the gain in simplification.

(5) Calculate Overall Time Weighted MOP for Each Migration Path. The final sub-step in this step is to use the time preference weights to determine an overall time weighted MOP figure for each of the migration paths identified in step two. This is accomplished by multiplying the MOP for all the periods in the useful life, by the time preference weight for that period, and then summing the resultants. This gives a single time weighted MOP for the migration path. This is likewise done for each migration path.

d. Develop and Apply Hierarchical Cost Model

The fourth step in the new framework is to develop and apply a hierarchical cost model to the target system and migratory paths established in steps one and two.

Figure 23 summarizes this step.

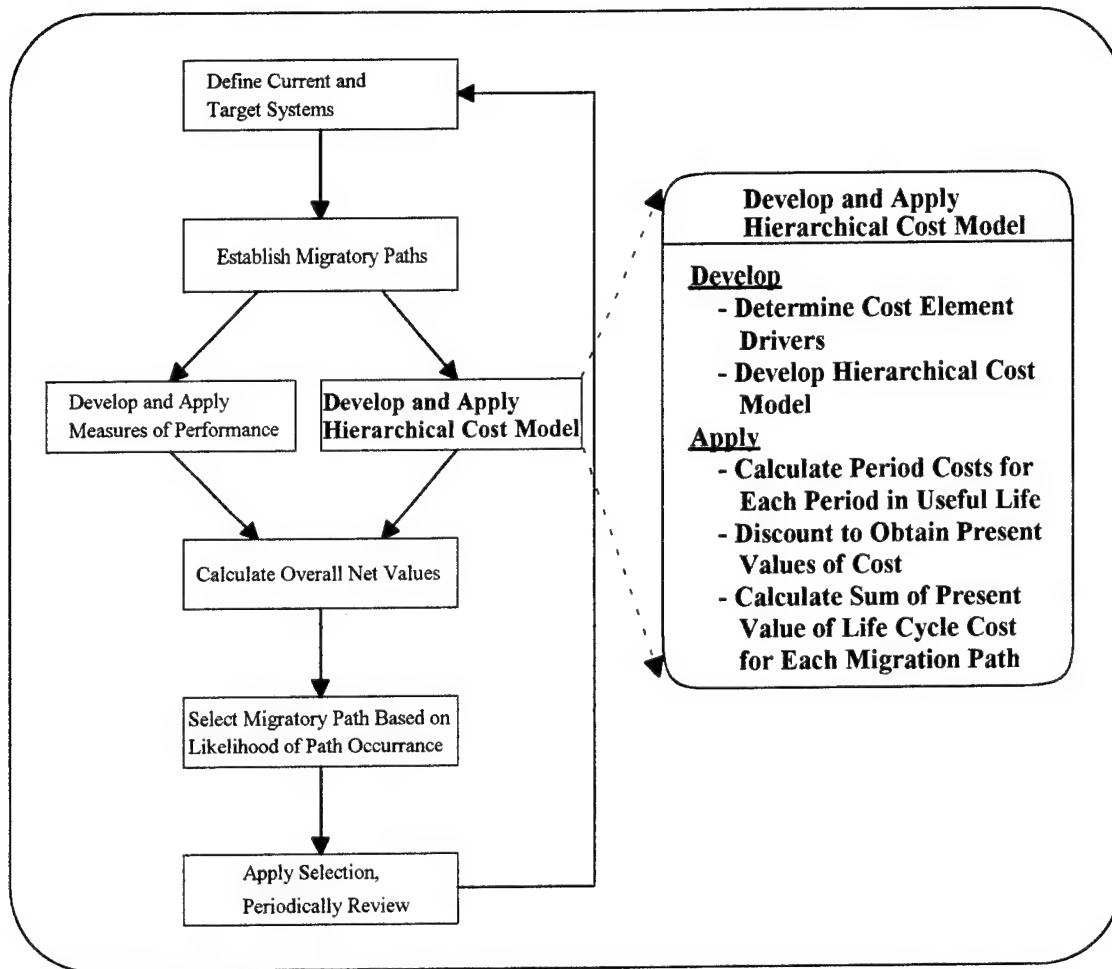


Figure 23 -- The New Framework - Step 4: Develop and Apply Cost Model

(1) Determine Cost Element Drivers. Before a cost model can be developed for the various migration paths, a list of cost element drivers for the card system must be identified. Like the list of performance attributes, this list should be as comprehensive as possible, and at this point the user should not be concerned with how the cost will be determined, how important the cost element is, or any other application concern. The goal of the first part of this sub-step is produce a comprehensive as possible list of cost elements.

(2) Develop Hierarchical Cost Model. Once the list of cost elements is established, it is helpful to graphically represent it in hierarchy form. This allows the grouping of some of the smaller cost elements into larger categories. Figure 24 provides a sample cost hierarchy. The user of this framework may generate their own cost hierarchy, or may apply the provided one to their problem. The reader will notice the category labeled *Application Specific Cost*, provided as a convenient place to add costs unique to their problem, including possible scrap values for previous system components.

(3) Calculate Costs for Each Period (Economic Forecasting as Necessary). The next sub-step is to apply this cost model to calculate the cost for each period in the useful life of the system. As was discussed in Chapter V, many things must be taken into account when determining the expected costs, especially in forecasting future costs.

(4) Discount Costs to Obtain the Present Value of Life Cycle Cost. Each of the period costs obtained in the previous sub-step's calculations, need to be discounted to obtain the present value of these costs. Discounting these costs, as was discussed in Chapter V, involves a trivial calculation. Present value costs must be compared in order to obtain the time weighted costs of the system.

(5) Calculate Present Value Life Cycle Cost for Each Migration Path. The final sub-step in this step is to calculate the overall present value life cycle costs for each migration path identified in step two. This value is simply the sum of all of the present value costs for each period in the useful life. Once this figure has been obtained, it is time to go on to the next step in the framework.

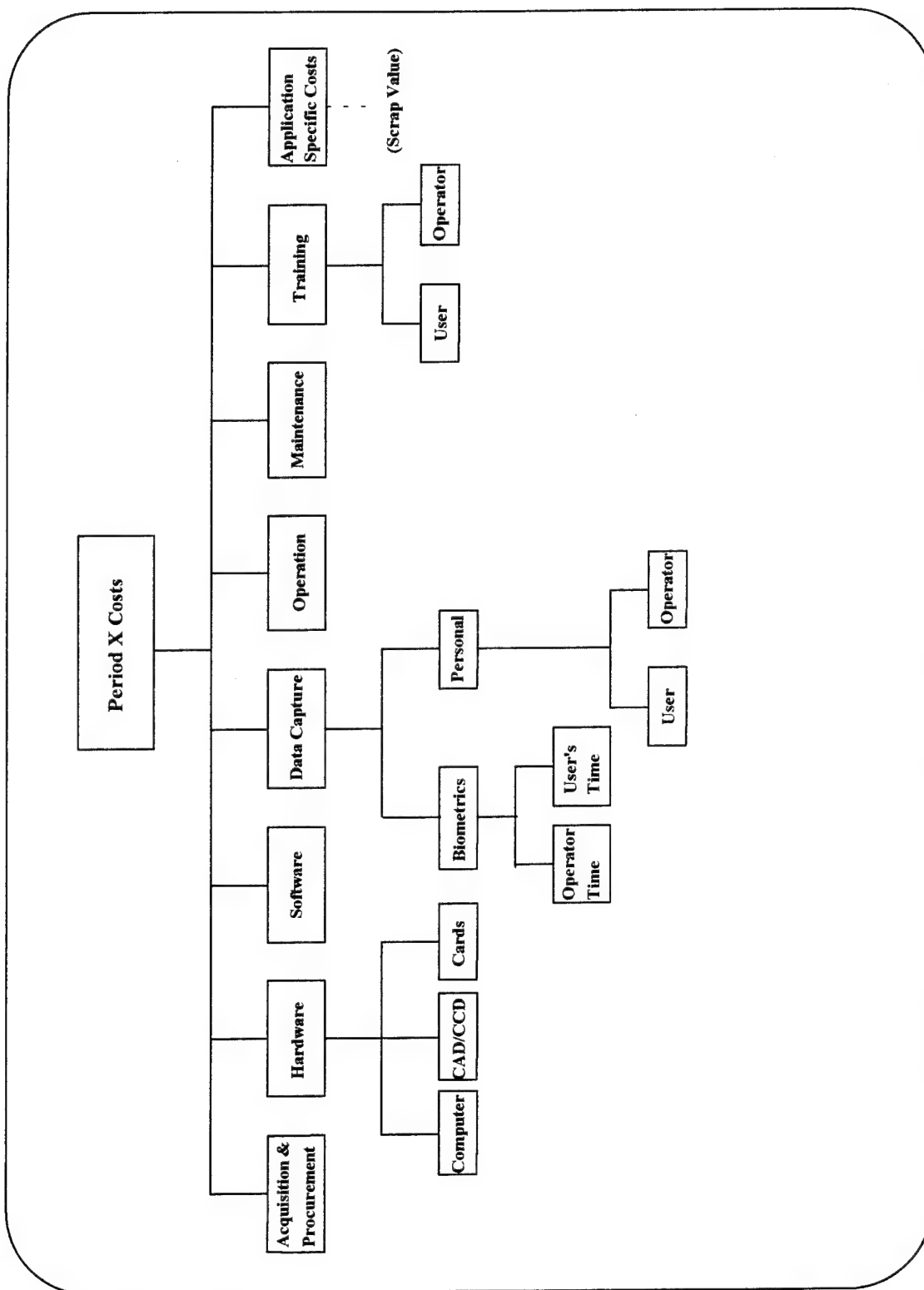


Figure 24 -- Cost Model Hierarchy

e. Calculate Overall Net Values

The fifth step in the framework is to calculate the overall net values of each migration path identified in step two. Figure 25 summarizes this step. This step has two sub-steps which are described below.

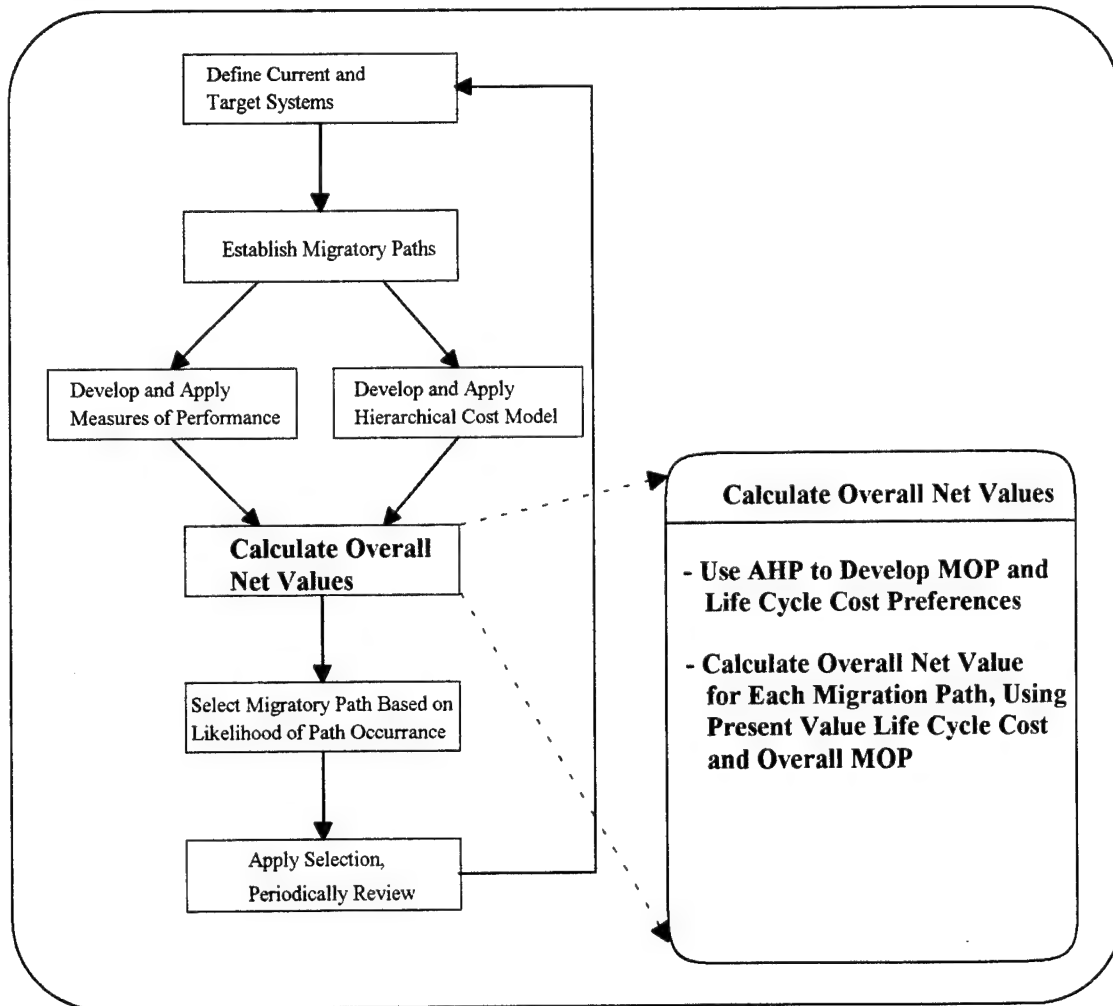


Figure 25 -- The New Framework - Step 5: Calculate Overall Net Values

(1) Use AHP to Develop MOP and Life Cycle Cost Preferences. The first sub-step involves determining the preference between cost and performance. As with any

cost-benefit analysis, a tradeoff between cost and performance must be made. AHP was again chosen as tool to weigh these preferences.

(2) Calculate Overall Net Values for Each Migration Path. After the cost and performance preference weights have been determined, the overall net value for each migration path can be determined. This is done using each migration path's time weighted MOP and present value life cycle costs, and multiplying them by their respective preference weight. While these numbers could be compared directly, a more intuitive comparison is possible by scaling one of the two figures to be of the same magnitude. This can be accomplished in one of two ways; scaling the measures of performance up from the double digits they are in, to the order of magnitude the costs are in, or scaling the costs down to the double digits the measures of performance are in. Using the first alternative, the user is then trading single dollars for very small (0.00001 on a million dollar system) increases in performance. The author found the later choice to be easier to conceptualize. If the present value costs for the system are in the tens of millions of dollars, the present value costs should be divided by one million before multiplying by the cost preference weight. The user will then have to remember that they are now trading millions of dollars for one unit increase in performance. After multiplication by their respective preference weights the value for cost is subtracted from the value for performance. The result is the overall net value for the migration path. This number may be negative or positive, depending on the values obtained for performance, the scaling used, and the preferences used. In either case, the larger the number the better the choice.

f. Select Migratory Path

The sixth step in the new framework is the selection of the migratory path.

Figure 26 provides a summary of this step. This step contains three sub-steps which are described below.

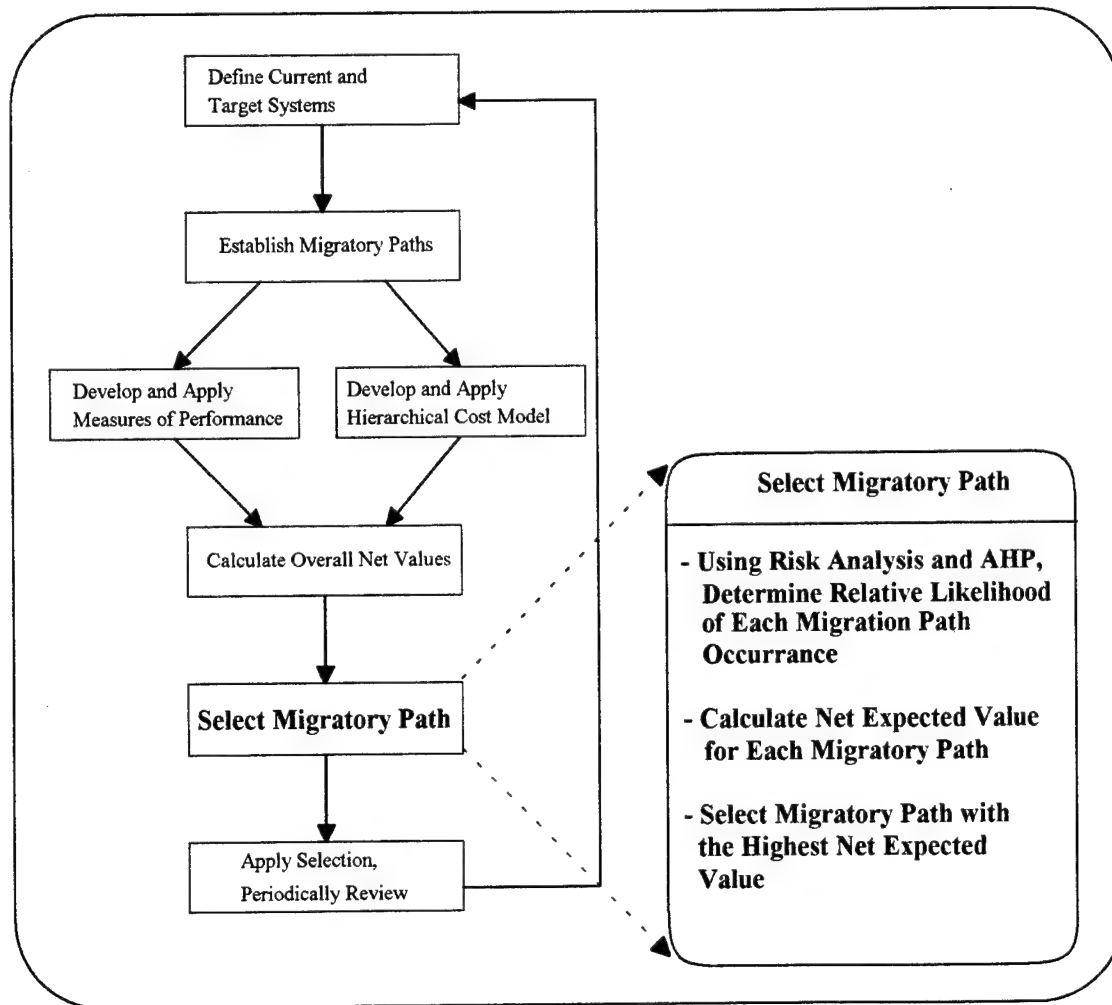


Figure 26 -- The New Framework - Step 6: Select Migratory Path

(1) Use Risk Analysis to Determine Likelihood of Path Occurrence. Since each of the migratory paths have some forecasting of future technological capabilities,

there is a likelihood of path occurrence associated with each path. The determination of these likelihood of path occurrences requires use of risk analysis as discussed in Chapter V. These likelihood's should be expressed as percentages, and do not need to add to one, however, they are more easily understood if normalized to add to one.

(2) Calculate Net Expected Value for Each Migration Path. Once the values for likelihood of path occurrence has been determined for each migration path identified in step two, the net expected value for the path can be determined. This is accomplished by multiplying the overall net values obtained in step five by the respective likelihood of occurrence value. In this manner, a net expected value, including consideration of the risk, is obtained for each migration path.

(3) Select Path with Greatest Net Expected Value. The net expected values calculated above are used to select the best solution to the problem. The path with the greatest net expected value, is the most appropriate solution to the problem, taking into account performance, cost, time, and technological risk.

g. Apply Selection and Reevaluate

The final step in the framework is the application and reevaluation of the selection. Figure 27 provides a summary of this step. The two sub-steps are described below.

(1) Initiate System Procurement. The first sub-step, is to initiate system procurement. Once the card technology selection has been made, the system must be defined, procured, installed, and operated. This paper does not discuss the procurement

of card technology systems in detail, however, it is worthwhile to remind the reader that there are many unique aspects of evolutionary system acquisition.

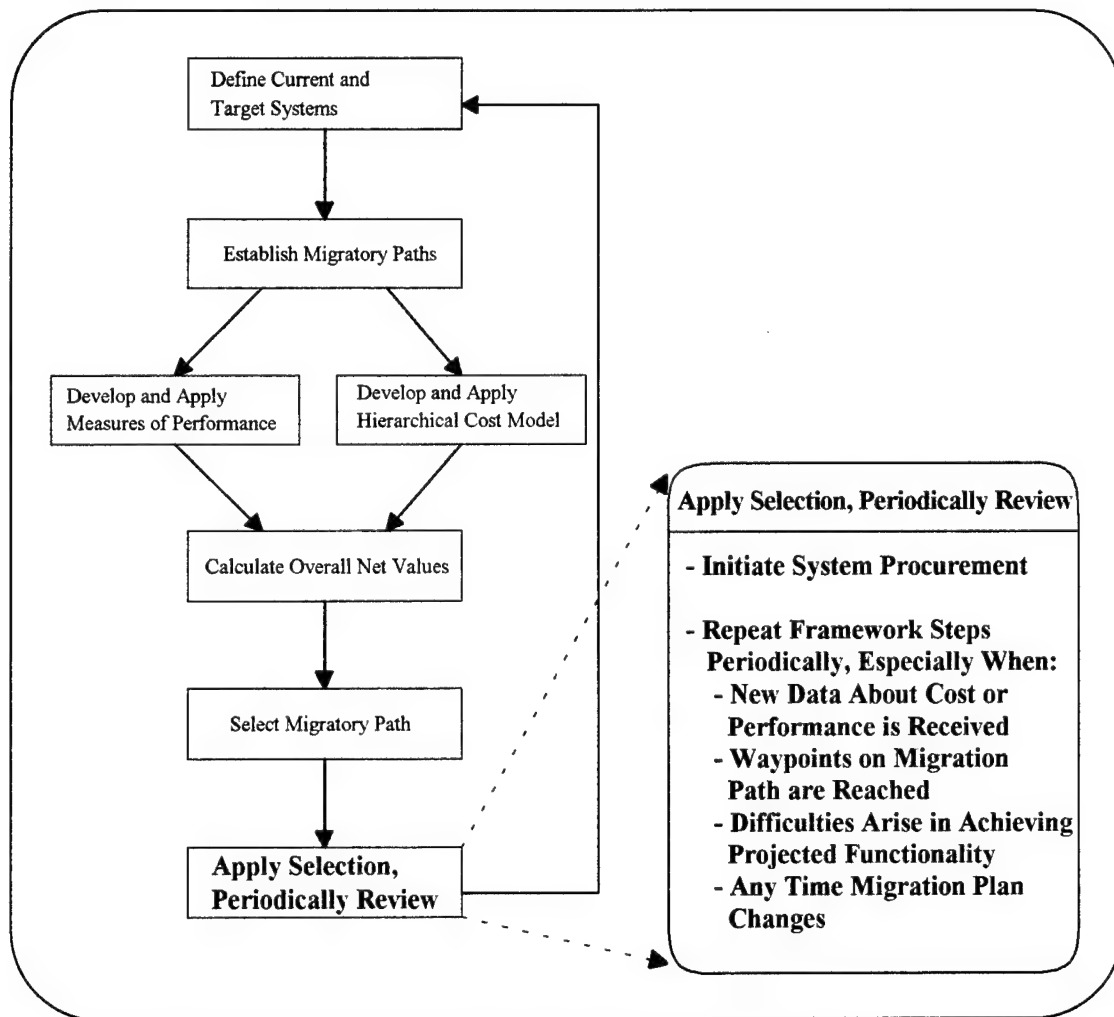


Figure 27 -- The New Framework - Step 7: Apply Selection, Periodically Review

(2) **Reevaluate New State Using Framework Steps.** The new framework is recursive in nature, and the card technology decision should be periodically reviewed. These reviews should occur whenever any of the following occur; new data about cost or performance is received, waypoints on migration path are reached (whether achieved or

not), difficulties arise in achieving projected functionality, or any time the migration plan changes. This is a crucial aspect of the new framework, as the framework is designed to be a continued evaluation tool, and not just an initial decision tool.

C. FRAMEWORK SUMMARY

The new framework presented in this chapter, provides the decision maker(s) with a functionally-oriented, capabilities-based approach to card technology systems analysis. Figure 28 provides summary of the decision tree for the new framework, complete with where the weights are applied. Appendix D provides an illustrative application of the new framework to an evolutionary card technology system.

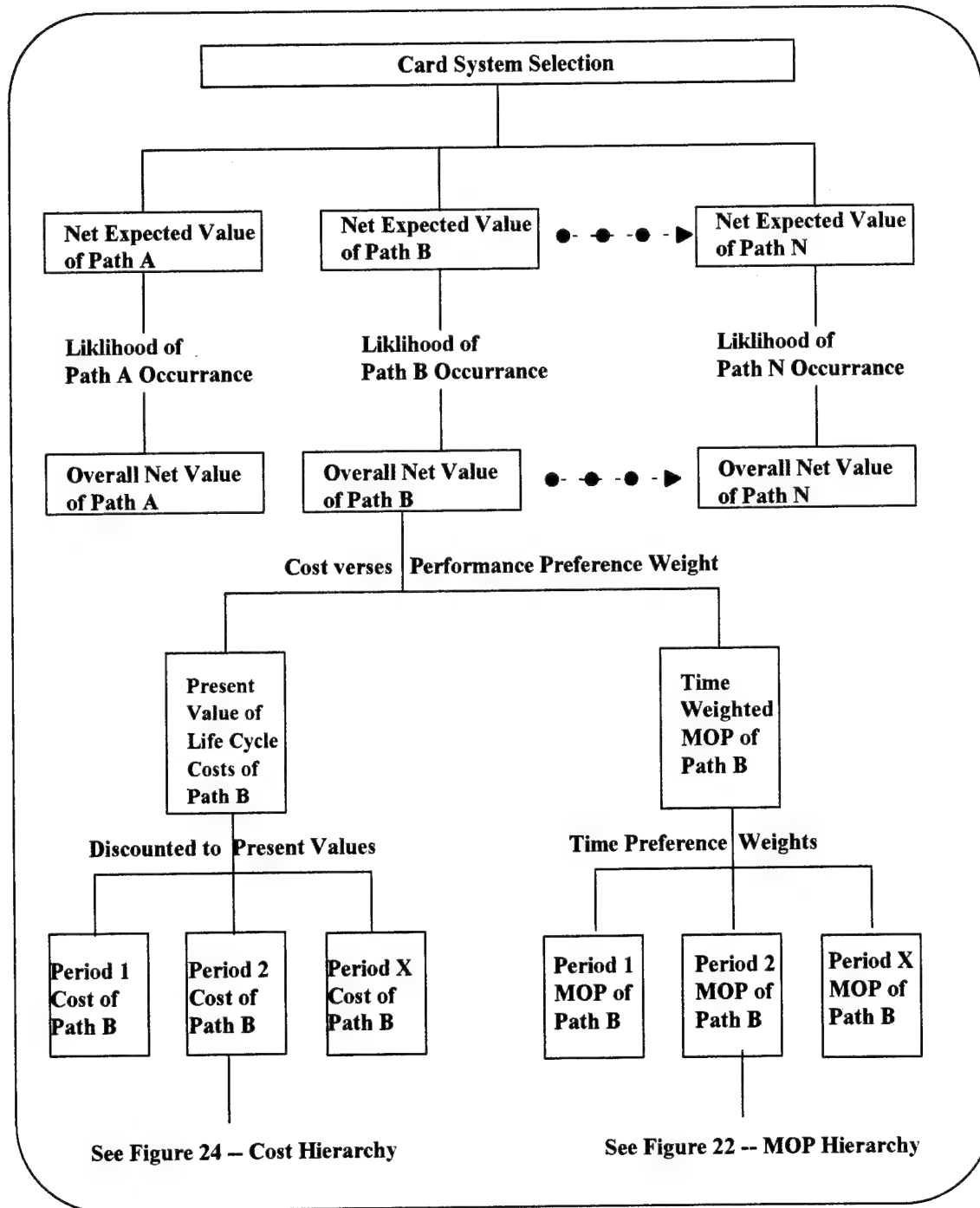


Figure 28 -- The New Framework Decision Hierarchy

VII. CONCLUSIONS AND RECOMMENDATIONS

A. SUMMARY

Chapter II presented a discussion of the 12 performance issues associated with card technology and authentication scheme selection. Available card technologies were presented in Chapter III, including the history, application, and uses of the technology. Authentication techniques were presented in Chapter IV, along with a discussion of authentication, identification, and error rates in general. Chapter V presented the DoD's view of and support for concepts used within the new framework, as well as a discussion of tools and theories employed within the framework. The new framework that focuses the evaluation of alternatives on their evolutionary upgrade paths was presented in Chapter VI. The framework presents a method that could be useful to decision makers in choosing between alternate card technology and authentication technique systems.

B. CONCLUSIONS

The following conclusions can be made in regard to card technology systems:

1. That card technology systems must capitalize on emerging technologies to gain the most benefit from technology.
2. That card technology systems can incorporate evolutionary upgrades throughout their useful life cycle, if procured through evolutionary acquisition.
3. The temporal component of card technology system procurement is an often overlooked aspect.

The new framework presented here offers an alternate approach to card system evaluations. The framework's methods for dealing with upgrade paths can be applied to any evolutionary system acquisition. Card technology systems will continue to change rapidly to keep up with state-of-the-art technology and security threats. This aspect, called the temporal component, must be evaluated by a system evaluation methodology. This framework accomplishes this. The author concludes that evaluations of alternatives can be based on cost/benefit analysis performed on the perceived future upgrade path alternatives.

While several different people using the same information and the new framework to the same problem, may come out with diverse results. However, it is the author's belief that the magnitudes will not significantly differ. The framework provides the user with a qualitative cost/benefit analysis of the perceived future upgrade path alternatives.

C. RECOMMENDATIONS

This framework represents an initial effort at basing the evaluation of alternative card technology systems on their future evolutionary upgrade paths. General concepts and procedures were introduced and applied to the card technology selection problem. Areas that could benefit from further research include:

1. More streamlined methods for determining target system functions and capabilities.
2. Methods that more accurately predict future upgrade technological capabilities and costs.

3. Methods that would more accurately evaluate the uncertainty and risk associated with migration path selection.
4. A more generic representation of the framework which could be applied to a variety of different systems acquisition challenges.

APPENDIX A: GLOSSARY OF ACRONYMS

ABS	Acrylonitrile Butadiene Styrene
ACS	Access Control System
AHP	Analytic Hierarchy Process
AIS	Automated Information System
AIT	Automated Information Technology
ANSC	American National Standards Committee
ANSI	American National Standards Institute
ATM	Automatic Teller Machine
BPI	Business Process Improvement or Bits Per Inch
BPR	Business Process Redesign
C4I	Command, Control, Communications, Computers and Intelligence
CAD	Card Acceptor Device
CCD	Card Coupling Device
CIM	Corporate Information Management
COS	Chip Operating System
COTS	Commercial-off-the-Shelf
CPU	Central Processing Unit
DEA	Data Encryption Algorithm
DES	Data Encryption Standard

DoD	Department of Defense
DRAW	Directly Read After Writing
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
EBT	Electronic Benefits Transfer
EEPROM (or E ² PROM)	Electronically Erasable Programmable Read-Only Memory
EFT	Electronic Funds Transfer
EM	Electro-magnetic
EMI	Electro-magnetic Interference
EPROM	Electronically Programmable Read-Only Memory
ETSI	European Telecommunications Standards Institute
FAR	False Acceptance Rate (type I error rate)
FRR	False Rejection Rate (type II error rate)
FTC	Financial Transaction Card (credit card)
GOTS	Government-off-the-Shelf
Hi-Co	High Coercivity (magnetic material)
IC	Integrated Circuit
ICC	Integrated Circuit Card
INTAMIC	International Association for Microcircuit Card
I/O	Input / Output
ISO	International Standards Organization

ITPB	Information Technology Policy Board
JEIDA	Japan Electronic Industry Development Association
JICSAP	Japan IC Card Application Council
KB	Kilo-byte (thousands of bytes)
Lo-Co	Low Coercivity (magnetic material)
LOS	Line of Sight
MB	Mega-byte (millions of bytes)
MCC	Memory Chip Card
MCOS	Multi-application Chip Operating System
MICR	Magnetic Ink Character Recognition
MOP	Measure of Performance
NIST	National Institute of Standards and Technology
OCR	Optical Character Recognition (or Reader)
OMC	Optical Memory Card
OS	Operating System
OSI	Open System Interconnection
PC	Personal Computer
PCMCIA	Personal Computer Memory Card International Association
Type I	3.3 mm thick
Type II	5.0 mm thick (slots will accept Type I also)
Type III	10.5 mm thick (slots will accept Type I or II also)
Type IV	15-18 mm thick in development, Toshiba proprietary
PIN	Personal Identification Number

PIV	Personal Identification Verification
POS	Point Of Sale
PROM	Programmable Read-Only Memory
PSC	Programmable Security Code
PV	Present Value
PVC	Poly Vinyl Chloride
PVCA	Poly Vinyl Chloride Acetate
RAM	Random Access Memory
RF	Radio Frequency
RFID or RF/ID	Radio Frequency Identification
ROM	Read-Only Memory
RSA	Rivest, Shamir, Adleman (algorithm for encryption)
TBACS	Token-Based Access Control Systems
UPC	Universal Product Code
WORM	Write Once Read Many

APPENDIX B: GLOSSARY OF TERMS

ABS	Acrylonitrile Butadiene Styrene - Plastic material frequently employed for injection molded cards.
Asymmetric Key	A cryptographic authentication technique in which the prover and verifier keys are different. Also called public and private key systems. Examples include RSA and DSS.
Authentication	The verification of a person or cards identity, given a claimed identity and an authentication measure. System matches input authentication against a stored reference for claimed identity to validate.
Bar Code	A series of vertical bars that contrast with the background. Usually black on white. These bars and spaces of specific widths are arranged in a unique sequential pattern to represent binary data.
Barium Ferrite	BaFe, permanent magnetic material "Read Only" placed in a card to form a binary code. Usually access control and financial transaction cards. A HiCo material..
Biometric	A method of using a permanent human attribute, physical or behavioral, for identification purposes. Example, fingerprints, voiceprints, eye retina patterns, hand geometry, and DNA.
Bit	A unit of information having only one of two values, a zero or a one. The units are used in combination to express information such as characters or digits.
Byte	A combination of bits (usually 8 to 10) that defines the representation of a set of characters or symbols.
CAD	Card Acceptor Device - a card reader for contact type cards, such as contact IC cards.
CCD	Card Coupling Device - a card reader for non-contact cards, such as proximity cards, RF/ID cards, and contactless IC cards.

Challenge-Response	A process where the verifier sends a value (challenge) to the prover, and expects a certain return value or information that is used to verify the authenticity of the prover.
Character	An alphabetic or numeric symbol.
Chip	A small square of thin, semiconductor material, such as silicon, that has been chemically processed to have a specific set of electrical characteristics such as circuits, storage, and/or logic elements.
Coercive Force	The energy required to saturate a given piece of magnetic material. Expressed in "Oersteds".
Coercivity	The magnetic "retention value" of different ferrous oxide materials. For example a high coercivity stripe will be less vulnerable to degaussing or erasure than a low coercivity stripe.
Contact	An electrical connecting surface between a Smart Card and its interfacing device that permits a flow of current.
Contactless	A connection between a Smart Card and its interfacing device that does not use a contact surface. In these devices a flow of current and signals is achieved by induction or high-frequency transmission techniques.
DEA	Data Encryption Algorithm - An encryption process that is a United States national standard, an ANSC national standard and a financial industry standard. The process is key-driven and reversible.
DES	Data Encryption Standard - a public domain encryption algorithm.
Disposable Card	A medium designed for a specific period or amount of use, such as the number of trips or telephone calls, after which the card no longer has any value and may be discarded.
DSS	Digital Signature Standard - An asymmetric key encryption standard widely used in the United States.
EEPROM	Electronically erasable, programmable, read-only memory. Chip memory which is electronically erasable and nonvolatile.

Embossing	A method of "striking" raised characters on plastic or metal. A male and female die set literally "squeeze" the material into a character shape.
Encryption	Converting clear or plain text to scrambled text with the use of a key driven algorithm.
EPROM	Electronically programmable, read-only memory. A semiconductor memory that is erasable with ultra-violet light. This is nonvolatile memory.
FAR	False Acceptance Rate - the average percentage of occurrence of false acceptance, authenticating a non-authentic prover. Also called type II error.
FRR	False Rejection Rate - the average percentage occurrence of rejection of an authentic user. Also called a type I error.
Ferrous Oxide	The metal "rust" particles that are used to make magnetic stripes. The controlled rusting (oxidation) determines the recording characteristics of the magnetic material. Also called Iron Oxide (Fe_2O_3) and is the most common LoCo material.
HiCo	High Coercivity - magnetic material which has properties allowing it to retain a greater amount of magnetic storage than LoCo material. Barium Ferrite (BaFe) most commonly used.
Hologram	Unique photo/graphic printing that gives the image a three dimensional effect. Usually employed for security or aesthetic effect.
Holographic	A method of encoding that embodies a three dimensional binary bit that is recognized a special reader.
Identification	The verification of identity given only the authentication method (no claimed identity). Much more difficult problem than authentication. System attempts to match input authentication with entire database of stored reference data.
ICC	Integrated Circuit Cards - a variety of different card types, all containing a single integrated circuit.

Iris Scan	A biometric authentication or identification technique in which the unique pattern of the iris of the eye is observed and recorded by a camera in the verifier.
LoCo	Low Coercivity - magnetic material which retains a lower amount of magnetic data than HiCo material. Iron Oxide (Fe ₂ O ₃) most commonly used.
LOS	Line of Sight - a direct, unobstructed path between the card acceptor device and the card itself.
OCR	Optical Character Recognition - Character fonts that are machine-readable by optical techniques.
Oersted	A unit of magnetic coercive force. Also used to define relative magnetic material "energy retention value".
OMC	Optical Memory Card - a card technology that uses optical media placed on the card to store data.
OSI	Open System Interconnection - An international standard for describing the interaction of computer systems through communications link characteristics by allocating the information functions into seven distinct layers.
Prover	A person or entity that is attempting to prove that it is a member in the system.
Proximity	A "non contact" system for reading cards. Data is exchanged between card and reader by Radio Frequency, Fiber Optics, Magnetic Induction, Laser or other non-mechanical contact technology.
PVC	Poly Vinyl Chloride - A material that is most frequently used in the manufacture of credit and I.D. cards. PVC has certain attributes that allow it to retain embossing. It is easily printable and will laminate at moderate temperatures.
Retinal Scan	A PIV technique based on an infrared scan of the eye retina.
RF	Radio Frequency that is used for a card to communicate with a reader in a "proximity" or "non-contact" system.

RSA	Rivest Shamir Adelman - an asymmetric key authentication scheme widely used in the United States.
Symmetric Key	A cryptographic authentication method where the key used for verifying is identical to the key used to generate the proof. Example is DES.
Verifier	An entity in the system that carries out the identification or authentication of the prover, and determines the authentication of the prover.
Voice Recognition	An authentication or identification technique which uses the unique flex, pitch, speed and other characteristics of voice to determine the authenticity of the prover.
WORM	Write Once Read Many - a memory type that is not re-writable.
Zero Knowledge	A challenge and response authentication protocol where the verifier is able to deduce that the prover holds the secret information, without having any knowledge of the secret information.

APPENDIX C: PERFORMANCE ATTRIBUTES SCALE

This appendix is intended to give the reader some additional sample performance attribute scales. These performance attribute scales are for the large categories of performance indicators provided in the sample measure of performance hierarchy in Figure 22. These large categories often encompass several aspects of card technology selection, and a performance attribute scale could be developed for each of the low level aspects. For purpose of illustration here, scales were developed for the large categories only, and the lower level aspects were used in the description of the level of performance.¹

Security Level

The security level consists of two parts, user and token authentication. The MOP scale will be the average of the values obtained for each

User Authentication: (has, knows, is)

- 1 none
- 2 Token
- 3 PIN
- 4 Password
- 5 Knowledge Challenge and Response
- 6 Combination Token and Knowledge
- 7 Behavioral Characteristic
- 8 Biometric Characteristic
- 9 Combination Knowledge and Characteristic
- 10 Characteristic Challenge and Response

Token Authentication:

- 1 none
- 2 Card size check
- 3 Card type check
- 4 Card knowledge (permanent) check (e.g. Wiegand)
- 5 Limited OS, data storage check
- 6 Encoded data only
- 7 Logic capable challenge and response
- 8 Full OS, data storage validation (logic capable)
- 9 Full cryptographic capable OS validation
- 10 Full cryptographic capable, interrogation exchange (card validates reader as well)

¹ Additional information on card technologies functionality matrix can be found in Bower, Leslie, "Automated Data Card Technologies: The Development of Functionality and Application Matrices, Naval Postgraduate School Thesis, September 1994.

User Acceptance: (fear of technology, fear of bodily damage, ease of use, fear of misuse)

- 1 Extremely Low - High fear levels, hard to use
- 2
- 3 Low - Moderate fear levels, not easy to use
- 4
- 5 Medium - Moderate fear levels, moderate ease of use
- 6
- 7 Medium High - Lower fear levels, fairly easy to use
- 8
- 9 High - Low fear levels, easy to use
- 10 Extremely High - No fear, easy to use

Memory (size, speed, life)

- 1 Low capacity (< 1 KB), slow transfer, short life (years) (e.g. magnetic stripe)
- 2
- 3 Moderate capacity (100's of KB), medium transfer rates, life in decades
- 4
- 5 Average capacity (> 1 KB, < 1 MB), medium transfer rates, life in decades
- 6
- 7
- 8 High capacity (> 1 MB), fast transfer rates, extremely long life (> 20 years)
- 9
- 10 Very high capacity (> 100 MB), fast transfer, unlimited life

Durability:

- 1 Poor - Easily damaged by multiple common items (such as water)
- 2
- 3 Fair - Fairly good durability against common handling, poor resistance to mishandling
- 4
- 5 Moderate - Good durability in common handling, resistant to abuse
- 6
- 7 Good - Very good durability in common handling, good resistance to abuse
- 8
- 9 Very good - Undamagable in normal handling, Very resistant to any damage
- 10 Extremely Good - virtually undamagable

Scalability/Expandability:

This measure of performance is more subjective than many of the other measures. A simple scale of 1-10 was developed and text description applied.

- | | |
|----|--|
| 1 | Poor - difficult to upgrade and expand |
| 2 | |
| 3 | Fair - not easy to upgrade and expand |
| 4 | |
| 5 | Moderately easy to upgrade and expand |
| 6 | |
| 7 | |
| 8 | Good - easy to upgrade and expand |
| 9 | |
| 10 | Excellent - easily upgraded and expanded |

Processing Ability

This consists of several indicators, speed of processing (MIPS), error detection, level of processing difficulty, operating system robustness and others.

- | | |
|----|---|
| 1 | No processing ability |
| 2 | Very limited processing ability - simple calculations and the like |
| 3 | |
| 4 | |
| 5 | Moderate - some processing ability (COS), low speed (1-10 MHz) |
| 6 | Average - advanced operating system (MCOS), low speed (1-10 MHz) |
| 7 | Good - advanced operating system, moderate speed (10-50 MHz) |
| 8 | |
| 9 | |
| 10 | Excellent, very high speed processing, complete sophisticated operating system, high speed (50-100 MHz) |

APPENDIX D: ILLUSTRATIVE EXAMPLE

This appendix is intended to give the reader a sample application of the framework steps in order to illustrate the steps of the new framework.

Step 1: Define Current and Target Systems

For this illustration a fairly simple target system was chosen in order to demonstrate the framework steps most clearly and not get the reader wrapped up in the technology considerations, nuances, and discussions of what is or is not yet possible in card technology systems. The target system is to be an organization wide access control system for installations, buildings, rooms, and computer systems. It is to be multi-biometric capable, and be able to carry out authentication and identification. It is to allow hands free operation and support a high speed of card travel (as in a vehicle). At this point a more in-depth analysis of the needs would be conducted, and a table of functionality versus technical capability, similar to Table 2, would be constructed. The current system would be analyzed as well. For simplicity, the current system of locks, guards, and manual access control measures were determined to be the base system. A planning horizon of 10 years was chosen to match that of the organization.

Step 2: Establish Migratory Paths

In-depth research would be required to establish viable migration paths toward the target system. However, a few possible migratory paths can be assumed. There are several waypoints possible in the migration toward the described system. The migration

breaks down into three major segments. In order of ease of solutions they are, the control of access to buildings and rooms, the control of access to computer systems, and the control of access to installations. Card systems to control access to buildings and rooms, is a well established, well vendor supported area with many technology choices.

Computer system control is less well established, however, there is considerable work being done in this field, and many of the same building access control technologies may be used. Mass vehicle access control to installations is not as common an application. Most installation access control system use similar technology to a building access control where a card is inserted, verified and a door or gate is opened to allow one individual or vehicle to pass. This is insufficient for control of mass access to an installation.

The first migratory path to be developed is a contactless programmable IC card system. These systems support many of the first segment's goals of room and building access. A system could be procured in the near term using contactless chip card system to handle most of these requirements. Access to computer systems using this system is possible in the near future as well. The use of contactless chip card systems for higher speed vehicle access control has not been proven as yet, however, this is a viable migratory path to assume it someday will be possible.

Another possible migratory path is a Wiegand technology based system. While Wiegand cards are not capable of the storage required to carry out stand alone biometric authentication, they could rely on a central database for all the access control information,

and just be used as an automatic data capture device. Again, if vehicle access control at speed is possible with Wiegand technology remains to be seen.

A third possible choice is some form of RF/ID or contactless memory only IC card system. This system would function using the data stored on the card as the reference data for authentication, and could support a decentralized system. This technology is being tested for use in automated toll collection and the like and appears promising to be able to carryout vehicle identification at speed.

Many other migratory paths could be developed, and a much more in-depth analysis of potential migratory paths would be required. However, these paths will be sufficient for an illustration of the framework.

Step 3: Develop and Apply Measures of Performance

The development and application of a measure of performance (MOP) hierarchy would be required next. The MOP hierarchy provided in the discussion of the new framework (Figure 22) will be used for this illustrative example as well. The next sub-step after developing the hierarchy is to weigh the importance of each MOP category. The development of a complete AHP analysis and weighing of the eight performance categories would be required. The complete pairwise comparisons required for these eight categories would not be a trivial item. In most cases a software package, such as Expert Choice by Decision Support Software, would be utilized. However, a sample of

the AHP pairwise comparisons and numerical ratings required is provided below to familiarize the user with the process.

The AHP can be used for weighing many different preference measures. It can be used for weighing the preference between two systems in terms of an attribute, or for weighing the importance of the attributes themselves. The standard AHP numerical rating scheme provided below is geared toward the weighing of preferences between two systems. Substituting the concept of importance for word preference below, gives a rating scale for the comparison of categories of performance.

<u>Verbal Judgment of Preference</u>	<u>Numerical Rating</u>
Extremely Preferred	9
Very Strongly to extremely	8
Very Strongly Preferred	7
Strongly to very strongly	6
Strongly Preferred	5
Moderately to strongly	4
Moderately preferred	3
Equally to moderately	2
Equally Preferred	1

To apply the AHP rating scale, each of the performance categories needs to be compared with each of the other categories. The first step is to define the goal of using the AHP.

Goal: SELECT THE BEST ACCESS CONTROL SYSTEM

With respect to the goal, comparing INTERFACE ROBUSTNESS to MEMORY

is INTERFACE ROBUSTNESS

Extremely Preferred	9
Very Strongly to extremely	8
Very Strongly Preferred	7
Strongly to very strongly	6

Strongly Preferred	5	to MEMORY
Moderately to strongly	4	
Moderately preferred	3	
Equally to moderately	2	
Equally Important	1	

This process would be continued until each of the categories were compared to each of the other categories. The result of these comparisons would be an eight by eight matrix of performance criteria preference (or importance). Using some mathematical manipulation, (carried out by the software package in this case) the matrix can be normalized and checked for consistency. The result is relative weights of importance of the eight performance criteria. For this illustration, the obtained weights for the performance criteria are as follows:

Interface Robustness	.237	
Memory	.035	
Processing	.035	
Security	.292	
Durability	.148	
User Acceptance	.045	
Scalability/Expandability	.208	
Application Specific MOP	<u>.000</u>	(no application specific MOPs)
	1.000	

The next sub-step is to calculate the aggregate MOP for each period. For this illustrative example, the planning horizon of 10 years was broken down into five two year periods. (periods of one year or 18 months could have been used, however this would have greatly expanded the size of the illustration). For each period and for each migration path, an aggregate MOP must be calculated. Using the MOP scales presented in Chapter VI and Appendix C, a value for MOP is calculated for each period. For example, for

contactless programmable IC card system (battery powered cards), period I, the MOP would look like:

Interface Robustness	5	
Memory	5	
Processing	5	
Security	8	
Durability	5	
User Acceptance	4	
Scalability/Expandability	6	
Application Specific MOP	<u>0</u>	(no application specific MOPs)
	38	

This would be completed for the programmable IC card system forecasted for periods II through V as well. The illustrative values for these periods are 46, 53, 61, and 69 respectively. This process would then be accomplished for the other migration paths as well.

The next sub-step would be to develop the time preference for performance. This is accomplished using AHP. As discussed in Chapter VI, this time preference is for the entire MOP, and not each individual category in the MOP. The AHP preference weights for each time period would be calculated using the same AHP described above. The weights used for the time periods in this illustrative example are:

<u>Time Period</u>	<u>Preference Weight</u>
I	0.30
II	0.22
III	0.18
IV	0.15
V	0.15

The next step is to calculate the overall time weighted MOP for each migration path. This is accomplished by multiplying the time period MOPs by the time period preferences. For the programmable IC card system this would be:

<u>Time Period</u>	<u>Preference Weight</u>	<u>MOP</u>	<u>Time Weighted MOP</u>
I	0.30	38	11.40
II	0.22	46	10.12
III	0.18	53	9.54
IV	0.15	61	9.15
V	0.15	69	<u>10.35</u>
			50.56

This would then be accomplished for each of the different migration paths.

Step 4: Develop and Apply Hierarchical Cost Model

A sample cost model was provided in Chapter VI, and will be used for this illustrative example as well. The determination of the costs of the system is unique to each individual procurement, and presenting an in-depth cost estimation at this point would be of limited use. The illustrative costs for each period for the contactless programmable IC card system is as follows, assuming a constant 10% interest rate.

<u>Time Period</u>	<u>Actual System Costs</u> (\$ millions)	<u>PV Costs</u> (\$ millions)
I	15.8	15.80
II	12.6	8.75
III	13.8	7.99
IV	16.2	7.81
V	18.7	<u>7.52</u>
		47.87

The present value costs for each migration path would be likewise calculated.

Step 5: Calculate Overall Net Values

To complete this step, a preference weighting between cost and performance must first be calculated. This is accomplished using AHP to compare the preference for cost versus performance. For this illustrative example, a 0.60 weighting is used for cost, and a 0.40 weighting is used for performance.

The next step is to obtain the overall net values for each migration path. As discussed in Chapter VI, this is accomplished by multiplying the MOP and cost numbers by their respective weights. For ease of understanding, the cost figure in this case is scaled to millions of dollars. Therefore the overall net value for the programmable contactless IC card system would be: $50.56 * (0.4) - 47.87 * (0.6) = - 8.498$

The overall net values for each of the other migration paths would be similarly calculated. The reader will note that the number obtained for the overall net value is negative. It may be positive or negative, depending on the figures obtained in the calculation, but in either case, the objective will be to obtain the largest number. That is either the smallest negative number, or the largest positive number.

Step 6: Select Migratory Path

The final calculation required is the determination of likelihood of path occurrence. This can be accomplished using AHP as discussed above and determining the relative likelihood of path occurrence, or by doing risk analysis and determining an actual figure (percentage) for the likelihood of path occurrence. Using risk analysis and normalizing the

resultant percentages to add to one, will provide similar figures to work with as the AHP results. Using these figures, a net expected value for each migration path is calculated. For example, if the likelihood of the programmable contactless IC card system reaching the target functionality is determined to be 0.54, the net expected value of that migration path would be $- 8.498 * 0.54 = - 4.59$. The net expected values obtained for each migration path are compared, and the migration path with the smallest negative or largest positive number is selected as the best alternative path taking into account performance, cost, time, and technological risk.

Step 7: Apply Selection and Reevaluate

After selection of a system has been made, the decision needs to be periodically reviewed. As discussed in Chapter VI, these reviews should occur periodically, whenever new information is received, and when waypoints are reached or missed. Three waypoints for this example could be building access, computer system access, and installation access. The expected time to functionality of each of these goals would be estimated at the outset of the project and periodically reviewed to ensure progress toward the waypoint.

BIBLIOGRAPHY

- Alexandre, Thomas and Vincent Cordonnier, "An Object-Oriented Approach for Implementing Biometrics in Smartcards," CardTech/SecurTech '94 Conference Proceedings, 1994, pp. 149-160.
- Allison, Graham and Gregory, Treverton, (eds.), Rethinking America's Security: Beyond Cold War to New World Order, W.W. Norton and Co., NY, NY, 1992.
- Anderson, D. R., D. J., Sweeney, and T. A., Williams, An Introduction To Management Science: Quantitative Approaches to Decision Making, 6th ed., West Publishing Co., St. Paul, MN, 1991.
- Anthes, Gary H., "Feds to Downsize With IT," ComputerWorld, Vol. 27, No. 37, September 13, 1993, p. 16.
- Arbel, A. and A., Seidmann, "Selecting a Microcomputer for Process Control and Data Acquisition," IIE Transactions, Vol. 16, No. 1, March 1984, pp. 73-80.
- Arrington, C. E., W., Hillison, and R. E., Jensen, "An Application of Analytical Hierarchy Process to Model Expert Judgments on Analytical Review Procedures," Journal of Accounting Research, Vol. 22, No. 1, Spring 1984, pp. 298-312.
- Bass, Peter, "Cards in Communication," Smart Card Technology International, 1994, p. 32.
- Bitter, Gary G., (ed.), Macmillan Encyclopedia of Computers, Macmillan, NY, NY, Vol. 2, 1992.
- Boehm, Barry, Software Engineering Economics, Prentice Hall, Englewood Cliffs, NJ, 1981.
- Bower, Leslie, "Automated Data Card (ADC) Technologies: The Development of Functionality and Application Matrices," Naval Postgraduate School Thesis, September 1994.
- Branscomb, Lewis M., et al., Empowering Technology: Implementing a U.S. Strategy, MIT Press, Cambridge, MA, 1993.

- Capaldi, Lucy, "The Defense Logistics Agency Automated Manifest System: A Status Report," CardTech/SecurTech '94 Conference Proceedings, 1994, pp. 293-304.
- Carter, Bob, "The Present and Future State of Biometric Technology," CardTech/SecurTech '94 Conference Proceedings, 1994, pp. 401-415.
- Casatelli, Christine, "Agencies Harness Smart-Card Power," Government Executive, Vol. 23, No. 7, July 1991, pp. 46-49.
- "The Chip Card: A New Data Carrier Made of Plastic," Smart Card Technology International, 1994, p. 50.
- Clinton, Bill J., President, and Albert Gore, Jr., Vice President, Technology for America's Economic Growth, A New Direction to Build Economic Strength, February 22, 1993.
- Corporate Information Management Process Improvement Methodology for DoD Functional Managers, 2nd ed., D. Appleton Company, Inc., Fairfax, VA, 1993.
- Defense Information Systems Agency, Center for Architecture, Department of Defense Technical Architecture Framework for Information Management (TAFIM), Ver. 2.0, November 1, 1993.
- Defense Information Systems Agency, Joint Interoperability and Engineering Organization, Center for Integration and Interoperability, DoD Information Integration Strategy "Tree" Diagrams (Vol. 1), Ver. 5, March 1994.
- Department of Transportation, Nontechnical Constraints and Barriers to Implementation of Intelligent Vehicle-Highway Systems, A Report to Congress, June 24, 1994.
- Department of the Treasury, Financial Management Service, Applications of Computer Card Technology, 1990.
- , Direct Payment Card: Mid-point Evaluation, March 31, 1993.
- , "Electric Benefit Transfer: Progress, Plans, Perspectives, and People," EBT Status Report, August 1992.
- Department of Defense, "Defense Acquisition," DoD Directive 5000.1, February 23, 1991.
- , "Defense Acquisition Management Policies and Procedures," DoD Instruction 5000.2, February 23, 1991.

- Dreifus, Henry, "Public Telephone Applications for Card Technologies; Practical Applications, Issues and Future Trends," CardTech '92 Conference Proceedings, 1992, pp. 3-18.
- , "North American Smart Card Activities 1993," CardTech/SecurTech '93 Conference Proceedings, 1993, p. 353-359.
- Driscoll, D. A., W. T., Lin, and P. R., Watkins, "Cost-Volume-Profit Analysis Under Uncertainty: A Synthesis and Framework for Evaluation," Journal of Accounting Literature, Vol. 3, Spring 1984, pp. 85-115.
- Dyer, J. S., "A Clarification of 'Remarks on the Analytic Hierarchy Process,'" Management Science, Vol. 36, No. 3, March 1990, pp. 274-275.
- , "Remarks on the Analytic Hierarchy Process," Management Science, Vol. 36, No. 3, March 1990, pp. 249-258.
- Dyer, James, Thomas Saaty, Patrick Harker, and Luis Vargas, "Discussion of AHP", Management Science, Vol. 36, No. 3, March 1990, pp. 247-275.
- Egge, Daniel Q., "A Framework for Evaluating Evolutionary Upgrade Paths of Command, Control and Communications Systems," Naval Postgraduate School Thesis, Monterey, CA, June 1993.
- Emshoff, J. R. and T. L. Saaty, "Applications of the analytic hierarchy process to long-range planning processes," European Journal of Operational Research, Vol. 10, No. 2, June 1982, pp. 131-143.
- GemPlus, Welcome to Smart Cards, draft copy, 1993.
- Girard, P.E., et. al, eds., "Modeling Choice Under Uncertainty in Military Systems Analysis," Technical Document 2216, Naval Ocean Systems Center, November 1991.
- Goldstein, T., S. P. Ladany, and A. Mehrez, "A Dual Replacement Model: A Note on Planning Horizon Procedures for Machine Replacements," Operations Research, Vol. 34 No. 6, November-December 1986, pp. 938-941.
- Gore, Albert, Vice President, Creating a Government That Works Better and Costs Less. Report of the National Performance Review, U.S. Government Printing Office, Washington, DC, September 7, 1993.

- Haga, William, J., and Robert Lang, "Revised Economic Analysis Procedures for ADP," Naval Postgraduate School Instruction Manual, Monterey, CA, January 1991.
- Haddock, Robert, "Building the Right Card Solution into Your Application," CardTech/SecurTech '93 Conference Proceedings, 1993, pp. 381-390.
- Harker, P. T., and L. G., Vargas, "Reply to 'Remarks on the Analytic Hierarchy Process' by J. S. Dyer," Management Science, Vol. 36, No. 3, March 1990, pp. 269-273.
- , "The Theory of Ratio Scale Estimation: Saaty's Analytic Hierarchy Process," Management Science, Vol. 33, No. 11, November 1987, pp. 1383-1403.
- Hirsch, Edward, BGen., USA (Ret.), "Evolutionary Acquisition of Command and Control Systems: Becoming a Reality," Signal, Vol. 42, No. 5, January 1988, pp. 23-26.
- Hollington, Jack, "Automated Fingerprint Analysis Offers Fast Verification," Sensor Review, Vol. 12, No. 3, March 1992, pp. 12-15.
- Holmes, James, P., "Promising Developments and Biometric Testing," CardTech/SecurTech '93 Conference Proceedings, 1993, pp. 317-322.
- Honold, Fred, "The Advantages of Contactless Cards," Smart Card Technology International, 1994, pp. 36-37.
- Howard, R. A., "Knowledge Maps," Management Science, Vol. 35 No. 8, August 1989, pp. 903-922.
- Information Spectrum, Inc., brochure, February 16, 1994.
- International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), International Standards:
 ISO/IEC 11693, Optical Memory Cards-General Characteristics, March 19, 1994
 ISO/IEC 11694, Optical Memory Cards - Linear Recording Method
 Part 1: Physical Characteristics, March 19, 1994.
 Part 2: Dimensions and Location of the Accessible Optical Area (Draft), September 22, 1993.
 Part 3: Optical Properties and Characteristics (Draft), November 11, 1993.
 Part 4: Logical Data Structures (Draft), November 11, 1993.
 ISO 7816 Smart Cards

- Kotheimer, William C., "A Database to Support DoD Business Process Redesign," Naval Postgraduate School Thesis, Monterey, CA, September 1992.
- Krueger, Julie, "Choosing the Right Chip For the Job," CardTech/SecurTech '94 Conference Proceedings, 1994, pp. 237-242.
- Kutchera, Arthur, "High Coercivity Media," CardTech '92 Conference Proceedings, 1992, pp. 33-54.
- Lavelle, Francis, "The Smart Card," Smart Card Technology International, 1994, p. 42.
- Linden, Larry F., "Introduction to Card Technology and Biometric Workshop," CardTech/SecurTech '93 Conference Proceedings, 1993, pp. 3-13.
- Mazara, Michael J., Military Technical Revolution: A Structural Framework, Center for Strategic and International Studies, Washington, D.C., March 1993.
- Miller, Benjamin, "Biometric Identification: The Power to Protect People, Places and Privacy," CardTech/SecurTech '94 Conference Proceedings, 1994, pp. 193-201.
- Modarres, M., What Every Engineer Should Know About Reliability and Risk Analysis, Marcel Dekker, Inc., NY, NY, 1992.
- Mos, Robert, "High Coercivity Encoding," CardTech '92 Conference Proceedings, 1992, pp. 55-72.
- Mourey, Richard, "Wiegand Card Technology Remains A Secure Investment," Security Technology and Design, Vol. 4, No. 6, August 1994, pp. 42-44.
- Muir, Barbara, "Authentication Considerations For External User Access," CardTech/SecurTech '93 Conference Proceedings, 1993, pp. 899-903.
- Naik, Jayant M., "Speaker Verification: A Tutorial," IEEE Communications Magazine, Vol. 28, No. 1, January 1990, pp. 40-47.
- Nelson, R.A., "Authentication Techniques For Smart Cards," CardTech/SecurTech '94 Conference Proceedings, 1994, pp. 47-60.
- Office of Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), "MARC Field Medical Workgroup, Medical Functional Integration Management Requirements and Deployable Systems," Washington, D.C., March 7, 1994.

Office of Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, Director of Defense Information, Status of the Department of Defense Corporate Information Management Initiative, Washington, D.C., October 27, 1992.

Office of Technology Assessment, United States Congress, Making Government Work, Government Printing Office, Washington, D.C., September 1993.

Ondrusch, Stephan, "Smallest and Fastest Implementation of Various Asymmetric Cryptographic Algorithms on Chip Cards," CardTech/SecurTech '94 Conference Proceedings, 1994, pp. 61-68.

Palmer, Roger C., The Bar Code Book: Reading, Printing, and Specification of Bar Code Symbols, 2nd ed., Helmers Publishing, Inc., Peterborough, NH, 1991.

Pemberton, James, "Contactless Cards --The Solution to All the Problems?", Smart Card Technology International, 1994, p. 85.

Peyret, Patrice, "RISC-Based, Next-Generation Smart Card Microcontroller Chips," CardTech/SecurTech '94 Conference Proceedings, 1994, pp. 9-36.

Pfleeger, Charles P., Security in Computing, Prentice Hall, Englewood Cliffs, NJ, 1989.

Powell, Colin L., Gen, USA, Chairman, Joint Chiefs of Staff, C4I For the Warrior, Washington, D.C., June 12, 1992.

Recognition Systems, Inc., ID3D HandKey Brochure, 1994.

Revillet, Marie and Mohammed Achemlal, "Biometric Authentication Principals, Use and Limitations," CardTech/SecurTech '94 Conference Proceedings, 1994, pp. 161-166.

Saaty, T. L., "A Scaling Method for Priorities in Hierarchical Structures," Journal of Mathematical Psychology, June 1977, pp. 234-281.

-----, The Analytic Hierarchy Process, McGraw-Hill, NY, NY, 1980.

-----, Decision Making for Leaders: The Analytic Hierarchy Process for Decisions in a Complex World, Lifetime Learning Publications, a Division of Wadsworth, Kansas City, KS, 1982.

-----, Prediction, Projection and Forecasting, Kluwer Academic Publishers, Boston, MA, 1993.

- Schneier, Bruce, Applied Cryptography: Protocols, Algorithms, and Source Code in C, Wiley and Sons, NY, NY, 1993.
- Schneider, J.K., "Ultrasound for Biometric Capture," CardTech/SecurTech '93 Conference Proceedings, 1993, pp. 333-338.
- Schoemaker, P. J. H. and C.C., Waid, "An Experimental Comparison of Different Approaches to Determining Weights in Additive Utility Models," Management Science, Vol. 28, No. 2, February 1982, pp. 182-196.
- Seidman, Stephan, "Advanced Card Technologies," CardTech/SecurTech '93 Conference Proceedings, 1993, pp. 19-25.
- , "The State of Smart Card Technology," CardTech/SecurTech '94 Conference Proceedings, 1994, pp. 205-213.
- Shachter, R. D., "Evaluating Influence Diagrams," Operations Research, Vol. 34 No. 6, November-December 1986, pp. 871-882.
- , and C.R., Kenley, "Gaussian Influence Diagrams," Management Science, Vol. 35, No. 5, May 1989, pp. 527-550.
- Sheppard, Colin, "A Neural Network Approach to Fingerprint Verification," CardTech/SecurTech '94 Conference Proceedings, 1994, pp. 183-190.
- Smart Card Technology International: The Global Journal of Advanced Card Technology, Smart Card Technology International Global Projects Group, 1994.
- "Smart Card Draws a Blank," New Scientist, Vol. 99, No. 1371, August 18, 1983, p. 456.
- The Smart Card Forum International Symposium Proceedings, Smart Card Forum, Washington, D.C., April 14, 1994.
- Sprague, Ralph H., Jr., and Barbara C. McNurlin, Information Systems In Practice, 3rd ed., Prentice Hall, Englewood Cliffs, NJ, 1993.
- Stanford, C.J., "Contactless Cards: An Overview," CardTech/SecurTech '93 Conference Proceedings, 1993, pp. 83-90.
- , "What is a Smart Card," CardTech/SecurTech '93 Conference Proceedings, 1993, pp. 115-126.

Svigals, Jerome, Smart Cards: The New Bank Cards, Macmillan Publishing Co., NY, NY, 1987.

Tolk, Keith M., "Random Patterns and Biometrics for Counterfeit Deterrence," CardTech/SecurTech '94 Conference Proceedings, 1994, pp. 141-147.

Toregas, Castis and Taly, Walsh, "Out With the Old, In With Re-engineering, American City & County, Vol. 108, No. 6, May 1993, pp. 49-56.

United States Congress, Office of Technology Assessment, Making Government Work: Electronic Delivery of Federal Services, Washington D.C., U.S. Government Printing Office, September, 1993.

Winkler, R. L., "Decision Modeling and Rational Choice: AHP and Utility Theory," Management Science, Vol. 36, No. 3, March 1990, pp. 247-248.

Won, Duk, J., "Introduction to Integrated Circuit (Smart) Cards," Program Management Review Paper, February 26, 1991.

Zahedi, Fatemeh, "The Analytic Hierarchy Process - A Survey of the Method and Its Applications," Interfaces, Vol. 16, No. 4, July-August 1986.

-----, "Data-Base Management System Evaluation and Selection Decisions," Decision Sciences, Vol. 16, No. 1, Winter 1985, pp. 91-116.

INITIAL DISTRIBUTION LIST

	No. Copies
1. Defense Technical Information Center Cameron Station Alexandria, VA 22304-6145	2
2. Library, Code 052 Naval Postgraduate School Monterey, CA 93943-5002	2
3. Roger Stemp Code CS/SP Naval Postgraduate School Monterey, CA 93943-5000	1
4. Professor Carl R. Jones Code SM/JS Naval Postgraduate School Monterey, CA 93943-5000	1
5. Professor Dan Boger Code SM/BO Naval Postgraduate School Monterey, CA 93943-5000	1
6. Professor William Kemple Code OR/KE Naval Postgraduate School Monterey, CA 93943-5000	1
7. Lt Joseph B. Spegele 6668 Suncrest Drive Roanoke, VA 24014	1
8. Mike Noll Information Technology Resources OASD (C3I) Room 1C255, Pentagon Washington, D.C. 20301	1

- | | |
|---|---|
| 9. John Moore
Dept. of the Treasury, Financial Management Service
Hyattsville, MD 20782 | 1 |
| 10. Mark Roboulet
HQ AFMC/LGT(AIT)
MITLA Program Manager
4375 Childlaw Road, Suite 6
Wright-Patterson AFB, OH 45433 | 1 |
| 11. Emilio Gonzalez
Office of Technology Assessment
Congress of the United States
Washington, D.C. 20510-8025 | 1 |
| 12. Major John J. Spegele, USMC
PM PLRS
SFAE-CM-ADDS-PLRS
Bldg. 2525
Ft. Monmouth, NJ 07703 | 1 |
| 13. United States Military Academy
Directorate of Information Management
Business Operations and Plans Division
West Point, NY 10996
Attn: Capt. Paul Logan | 1 |